

(corresponding to
US 2004/0006703 A1)

22

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-173215

(43)Date of publication of application : 20.06.2003

(51)Int.Cl.

G06F 1/00
G06F 12/14
G09C 1/00
H04L 9/32

(21)Application number : 2002-145264

(71)Applicant : SONY CORP

(22)Date of filing : 20.05.2002

(72)Inventor : KITANI SATOSHI
MORIKAZU MUNETOSHI

(30)Priority

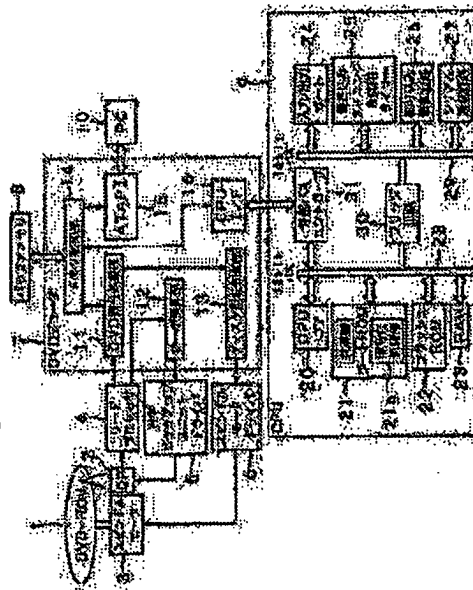
Priority number : 2001294506 Priority date : 26.09.2001 Priority country : JP

(54) INFORMATION PROCESSOR, PROGRAM LOADING METHOD, RECORDING MEDIUM,
PROGRAM UPDATING METHOD AND CIRCUIT ELEMENT

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent leakage of
program data during a program update.

SOLUTION: A control part 9 is provided with a ciphered
program data receiving part 31 receiving ciphered
program data of a second program ciphered by a
predetermined cipher key in response to a program
update request requesting update of a first program, a
deciphering part 21a deciphering the ciphered program
data received by the ciphered program data receiving
part 31 into the second program by using a
predetermined decipher key, program writing parts 20
and 21 writing the second program deciphered from the
ciphered program data by the deciphering part 21a into a
storing part 22, and a fetch limiting part 31 limiting
fetching of the second program deciphered by the
deciphering part 21a and the second program written in
the storing part 22 from an external device.



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-173215

(P2003-173215A)

(43)公開日 平成15年6月20日(2003.6.20)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード*(参考)
G 0 6 F 1/00		G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
	12/14	G 0 9 C 1/00	6 4 0 D 5 B 0 7 6
G 0 9 C 1/00	6 4 0	G 0 6 F 9/08	6 6 0 L 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 A

審査請求 未請求 請求項の数81 O L (全 33 頁)

(21)出願番号 特願2002-145264(P2002-145264)
 (22)出願日 平成14年5月20日(2002.5.20)
 (31)優先権主張番号 特願2001-294506(P2001-294506)
 (32)優先日 平成13年9月26日(2001.9.26)
 (33)優先権主張国 日本(J P)

(71)出願人 000002185
 ソニー株式会社
 東京都品川区北品川6丁目7番35号
 (72)発明者 木谷 聡
 東京都品川区北品川6丁目7番35号 ソニー株式会社内
 (72)発明者 盛一 宗利
 東京都品川区北品川6丁目7番35号 ソニー株式会社内
 (74)代理人 100067736
 弁理士 小池 晃 (外2名)

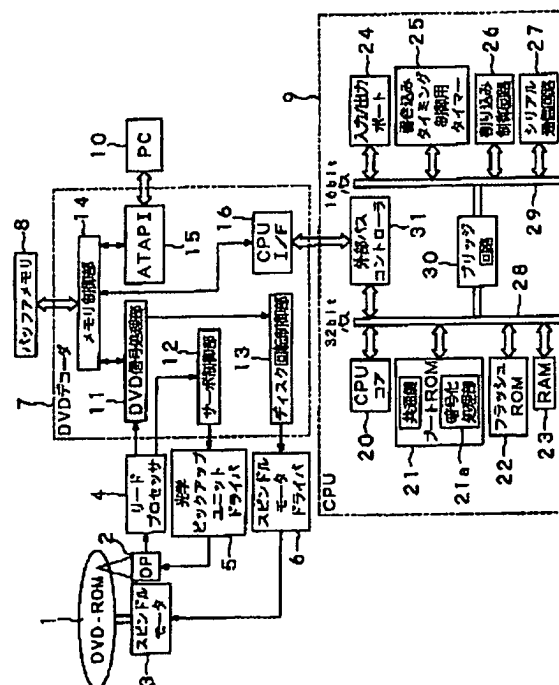
最終頁に続く

(54)【発明の名称】 情報処理装置、プログラムロード方法、記録媒体、プログラム更新方法及び回路素子

(57)【要約】

【課題】 プログラム更新時のプログラムデータの漏洩を防止する。

【解決手段】 制御部9は、第1のプログラムの更新を要求するプログラム更新要求に応じて、第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信部31と、暗号化プログラムデータ受信部31で受信した暗号化プログラムデータを所定の復号鍵を用いて第2のプログラムに復号する復号部21aと、復号部21aで暗号化プログラムデータから復号された第2のプログラムを、記憶部22に書き込むプログラム書き込み部20、21と、復号部21aで復号された第2のプログラム及び記憶部22に書き込まれた第2のプログラムの外部装置からの取り出しを制限する取り出し制限部31とを備えることで実現する。



【特許請求の範囲】

【請求項1】 所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、

上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号手段と、

上記復号手段で上記暗号化プログラムデータから復号された上記所定のプログラムを記憶する記憶手段と、

上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出し手段と、

上記読み出し手段によって読み出された上記所定のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを備えることを特徴とする情報処理装置。

【請求項2】 上記暗号化プログラムデータ受信手段は、外部装置から送信される暗号化プログラムデータを受信することを特徴とする請求1記載の情報処理装置。

【請求項3】 上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生手段を備え、

上記暗号化プログラムデータ受信手段は、上記再生手段で再生された上記暗号化プログラムデータを受信することを特徴とする請求項1記載の情報処理装置。

【請求項4】 上記暗号化プログラムデータが記憶された暗号化プログラムデータ記憶手段を備え、上記暗号化プログラムデータ記憶手段に記憶されている上記暗号化プログラムデータを読み出す暗号化プログラムデータ読み出し手段と、

上記暗号化プログラムデータ受信手段は、上記暗号化プログラムデータ読み出し手段によって読み出された上記暗号化プログラムデータを受信することを特徴とする請求項1記載の情報処理装置。

【請求項5】 上記暗号化プログラムデータ受信手段で受信される暗号化プログラムデータは、上記所定のプログラムのプログラムデータから所定の演算によって算出された第1の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含むことを特徴とする請求項1記載の情報処理装置。

【請求項6】 上記復号手段は、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第1の検証データと、上記検証プログラムに復号し、上記記憶手段は上記復号手段で復号された上記第1の検証データと、上記検証プログラムとを記憶し、

上記制御手段は、上記所定のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記所定のプログラムのプログラムデータから

第2の検証データを算出し、算出された上記第2の検証データと、上記記憶手段に記憶されている上記第1の検証データとを比較し、

上記読み出し手段は、上記制御手段によって比較された上記第1の検証データと、上記第2の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記所定のプログラムを読み出すことを特徴とする請求項5記載の情報処理装置。

【請求項7】 情報処理装置に所定のプログラムをロードするためのプログラムロード方法であって、上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、

上記暗号化プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号ステップと、

上記復号ステップで上記暗号化プログラムデータから復号された上記所定のプログラムを記憶手段に記憶する記憶ステップと、

上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出しステップと、

上記読み出しステップによって読み出された上記所定のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御ステップとを備えることを特徴とするプログラムロード方法。

【請求項8】 上記暗号化プログラムデータ受信ステップは、外部装置から送信される暗号化プログラムデータを受信することを特徴とする請求7記載のプログラムロード方法。

【請求項9】 上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生ステップを備え、

上記暗号化プログラムデータ受信ステップは、上記再生ステップで再生された上記暗号化プログラムデータを受信することを特徴とする請求項7記載のプログラムロード方法。

【請求項10】 上記暗号化プログラムデータが記憶されている当該情報処理装置に備えられた暗号化プログラムデータ記憶手段から上記暗号化プログラムデータを読み出す暗号化プログラムデータ読み出しステップを備え、

上記暗号化プログラムデータ受信ステップは、上記暗号化プログラム読み出しステップによって読み出された上記暗号化プログラムデータを受信することを特徴とする請求項7記載のプログラムロード方法。

【請求項11】 上記暗号化プログラムデータ受信ステップは、上記所定のプログラムのプログラムデータから所定の演算によって算出された第1の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データ

と、暗号化検証プログラムとを含んだ上記暗号化プログラムデータを受信することを特徴とする請求項 7 記載のプログラムロード方法。

【請求項 12】 上記復号ステップは、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第 1 の検証データと、上記検証プログラムに復号し、

上記記憶ステップは、上記記憶手段に上記復号ステップで復号された上記第 1 の検証データと、上記検証プログラムとを記憶し、

上記制御ステップで、上記所定のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記所定のプログラムのプログラムデータから第 2 の検証データを算出する検証データ算出ステップと、

上記検証データ算出ステップで算出された上記第 2 の検証データと、上記記憶手段に記憶されている上記第 1 の検証データとを比較する検証データ比較ステップとを備え、

上記読み出しステップは、上記検証データ比較ステップによって比較された上記第 1 の検証データと、上記第 2 の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記所定のプログラムを読み出すことを特徴とする請求項 11 記載のプログラムロード方法。

【請求項 13】 情報処理装置に所定のプログラムをロードするためのプログラムを記録した記録媒体であって、

上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、

上記暗号化プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号ステップと、上記復号ステップで上記暗号化プログラムデータから復号された上記所定のプログラムを記憶手段に記憶する記憶ステップと、

上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出しステップと、

上記読み出しステップによって読み出された上記所定のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御ステップとを備えることを特徴とするプログラムを記録した記録媒体。

【請求項 14】 上記暗号化プログラムデータ受信ステップは、外部装置から送信される暗号化プログラムデータを受信することを特徴とするプログラムを記録した請求項 13 記載の記録媒体。

【請求項 15】 上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生ステップを備え、

上記暗号化プログラムデータ受信ステップは、上記再生ステップで再生された上記暗号化プログラムデータを受信することを特徴とするプログラムを記録した請求項 13 記載の記録媒体。

【請求項 16】 上記暗号化プログラムデータが記憶されている当該情報処理装置に備えられた暗号化プログラムデータ記憶手段から上記暗号化プログラムデータを読み出す暗号化プログラムデータ読み出しステップを備え、

上記暗号化プログラムデータ受信ステップは、上記暗号化プログラム読み出しステップによって読み出された上記暗号化プログラムデータを受信することを特徴とするプログラムを記録した請求項 13 記載の記録媒体。

【請求項 17】 上記暗号化プログラムデータ受信ステップは、上記所定のプログラムのプログラムデータから所定の演算によって算出された第 1 の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含んだ上記暗号化プログラムデータを受信することを特徴とするプログラムを記録した請求項 13 記載の記録媒体。

【請求項 18】 上記復号ステップは、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第 1 の検証データと、上記検証プログラムに復号し、

上記記憶ステップは、上記記憶手段に上記復号ステップで復号された上記第 1 の検証データと、上記検証プログラムとを記憶し、

上記制御ステップで、上記所定のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記所定のプログラムのプログラムデータから第 2 の検証データを算出する検証データ算出ステップと、

上記検証データ算出ステップで算出された上記第 2 の検証データと、上記記憶手段に記憶されている上記第 1 の検証データとを比較する検証データ比較ステップとを備え、

上記読み出しステップは、上記検証データ比較ステップによって比較された上記第 1 の検証データと、上記第 2 の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記所定のプログラムを読み出すことを特徴とするプログラムを記録した請求項 17 記載の記録媒体。

【請求項 19】 第 1 のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第 1 のプログラムを読み出し、読み出した上記第 1 のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置であって、

上記制御部は、

上記第1のプログラムの更新を要求するプログラム更新要求に応じて、第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、

上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記第2のプログラムに復号する復号手段と、

上記復号手段で上記暗号化プログラムデータから復号された第2のプログラムを、上記記憶手段に書き込むプログラム書き込み手段と、

上記復号手段で復号された第2のプログラム及び上記記憶手段に書き込まれた第2のプログラムの外部装置からの取り出しを制限する取り出し制限手段とを備えることを特徴とする情報処理装置。

【請求項20】 上記暗号化プログラムデータ受信手段は、外部装置から送信される暗号化プログラムデータを受信することを特徴とする請求項19記載の情報処理装置。

【請求項21】 上記第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生手段を備え、

上記制御手段は、上記プログラム更新要求に応じて、上記記録媒体を再生させるよう上記再生手段を制御し、

上記暗号化プログラムデータ受信手段は、上記再生手段で再生された上記暗号化プログラムデータを受信することを特徴とする請求項19記載の情報処理装置。

【請求項22】 上記暗号化プログラムデータ受信手段で受信される暗号化プログラムデータは、上記第2のプログラムのプログラムデータから所定の演算によって算出された第1の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含むことを特徴とする請求項19記載の情報処理装置。

【請求項23】 上記復号手段は、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第1の検証データと、上記検証プログラムに復号し、上記プログラム書き込み手段は、上記復号手段で復号された上記第1の検証データと、上記検証プログラムとを上記記憶手段に書き込み、

上記制御手段は、上記第2のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記第2のプログラムのプログラムデータから第2の検証データを算出し、算出された上記第2の検証データと、上記記憶手段に記憶されている上記第1の検証データとを比較し、比較した上記第1の検証データと、上記第2の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記第2のプログラムを読み出すことを特徴とする請求項22記載の情報処理装

置。

【請求項24】 第1のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第1のプログラムを読み出し、読み出した上記第1のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置のプログラム更新方法であって、

上記第1のプログラムの更新を要求するプログラム更新要求に応じて、第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、

上記受信した暗号化プログラムデータを所定の復号鍵を用いて上記第2のプログラムに復号する復号ステップと、

上記復号された第2のプログラムの外部装置からの取り出しを制限する取り出し制限ステップと、

上記暗号化プログラムデータから復号された第2のプログラムを、上記記憶手段に書き込むプログラム書き込みステップとを備えることを特徴とするプログラム更新方法。

【請求項25】 上記暗号化プログラムデータ受信ステップでは、外部装置から送信される暗号化プログラムデータを受信することを特徴とする請求項24記載のプログラム更新方法。

【請求項26】 上記第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生ステップを備え、

上記再生ステップは、上記プログラム更新要求を受信したことに応じて上記記録媒体を再生させ、

上記暗号化プログラムデータ受信ステップは、上記再生された暗号化プログラムデータを受信することを特徴とする請求項24記載のプログラム更新方法。

【請求項27】 上記暗号化プログラムデータ受信ステップは、上記第2のプログラムのプログラムデータから所定の演算によって算出された第1の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含んだ上記暗号化プログラムデータを受信することを特徴とする請求項24記載のプログラム更新方法。

【請求項28】 上記復号ステップは、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第1の検証データと、上記検証プログラムに復号し、

上記プログラム書き込みステップは、上記復号ステップで復号された上記第1の検証データと、上記検証プログラムとを上記記憶手段に書き込み、

上記制御手段で上記第2のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶さ

れた上記第2のプログラムのプログラムデータから第2の検証データを算出する検証データ算出ステップと、上記検証データ算出ステップで算出された上記第2の検証データと、上記記憶手段に記憶されている上記第1の検証データとを比較する検証データ比較ステップと、上記検証データ比較ステップによって比較された上記第1の検証データと、上記第2の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記第2のプログラムを読み出すプログラム読み出しステップとを備えることを特徴とする請求項27記載のプログラム更新方法。

【請求項29】 第1のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第1のプログラムを読み出し、読み出した上記第1のプログラムに基づいて所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置の上記第1のプログラムを更新するためのプログラムを記録した記録媒体であって、上記第1のプログラムの更新を要求するプログラム更新要求に応じて、第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、上記受信した暗号化プログラムデータを所定の復号鍵を用いて上記第2のプログラムに復号する復号ステップと、上記復号された第2のプログラムの外部装置からの取り出しを制限する取り出し制限ステップと、上記暗号化プログラムデータから復号された第2のプログラムを上記記憶手段に書き込むプログラム書き込みステップとを備えることを特徴とするプログラムを記録した記録媒体。

【請求項30】 上記暗号化プログラムデータ受信ステップでは、外部装置から送信される暗号化プログラムデータを受信することを特徴とするプログラムを記録した請求項29記載の記録媒体。

【請求項31】 上記第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された当該記録媒体を再生する再生ステップを備え、上記再生ステップは、上記プログラム更新要求を受信したことに応じて当該記録媒体に記録されている上記暗号化プログラムデータを再生させ、上記暗号化プログラムデータ受信ステップは、上記再生された上記暗号化プログラムデータを受信することを特徴とするプログラムを記録した請求項29記載の記録媒体。

【請求項32】 上記暗号化プログラムデータ受信ステップは、上記第2のプログラムのプログラムデータから所定の演算によって算出された第1の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含んだ上記暗号化プロ

ラムデータを受信することを特徴とするプログラムを記録した請求項29記載の記録媒体。

【請求項33】 上記復号ステップは、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第1の検証データと、上記検証プログラムに復号し、

上記プログラム書き込みステップは、上記復号ステップで復号された上記第1の検証データと、上記検証プログラムとを上記記憶手段に書き込み、

上記制御手段で上記所定のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記所定のプログラムのプログラムデータから第2の検証データを算出する検証データ算出ステップと、算出された上記第2の検証データと、上記記憶手段に記憶されている上記第1の検証データとを比較する検証データ比較ステップと、

上記検証データ比較ステップによって比較された上記第1の検証データと、上記第2の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記第2のプログラムを読み出すプログラム読み出しステップとを備えることを特徴とするプログラムを記録した請求項32記載の記録媒体。

【請求項34】 第1のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第1のプログラムを読み出し、読み出した上記第1のプログラムに基づいて情報処理装置の所定の動作を制御する制御手段とを集積化した回路素子であって、

上記第1のプログラムの更新を要求するプログラム更新要求に応じて、第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、

上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記第2のプログラムに復号する復号手段と、

上記復号手段で上記暗号化プログラムデータから復号された第2のプログラムを、上記記憶手段に書き込むプログラム書き込み手段と、

上記復号手段で復号された第2のプログラム及び上記記憶手段に書き込まれた第2のプログラムの外部装置からの取り出しを制限する取り出し制限手段とを集積化してなることを特徴とする回路素子。

【請求項35】 上記暗号化プログラムデータ受信手段は、外部装置から送信される暗号化プログラムデータを受信することを特徴とする請求項34記載の回路素子。

【請求項36】 上記第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生手段を備えた情報処理装置に備えられ、

上記制御手段は、上記プログラム更新要求に応じて、上

記録媒体を再生させるよう上記再生手段を制御し、上記暗号化プログラムデータ受信手段は、上記情報処理装置の再生手段で再生された上記暗号化プログラムデータを受信することを特徴とする請求項3記載の回路素子。

【請求項37】 上記暗号化プログラムデータ受信手段で受信される暗号化プログラムデータは、上記第2のプログラムのプログラムデータから所定の演算によって算出された第1の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含むことを特徴とする請求項34記載の回路素子。

【請求項38】 上記復号手段は、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第1の検証データと、上記検証プログラムに復号し、上記プログラム書き込み手段は、上記復号手段で復号された上記第1の検証データと、上記検証プログラムとを上記記憶手段に書き込み、

上記制御手段は、上記第2のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記第2のプログラムのプログラムデータから第2の検証データを算出し、算出された上記第2の検証データと、上記記憶手段に記憶されている上記第1の検証データとを比較し、比較した上記第1の検証データと、上記第2の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記第2のプログラムを読み出すことを特徴とする請求項37記載の回路素子。

【請求項39】 第1のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第1のプログラムを読み出し、読み出した上記第1のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置であって、上記第1のプログラムの更新を要求するプログラム更新要求に応じて、第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、

上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記第2のプログラムに復号する復号手段と、

上記復号手段で上記暗号化プログラムデータから復号された上記第2のプログラムを上記制御部に送信するプログラム送信手段とを備え、

上記制御部は、上記送信手段によって送信された上記第2のプログラムを受信するプログラム受信手段と、上記プログラム受信手段で受信した上記第2のプログラムを上記記憶手段に書き込むプログラム書き込み手段とを有することを特徴とする情報処理装置。

【請求項40】 上記暗号化プログラムデータ受信手段

は、外部装置から送信される暗号化プログラムデータを受信することを特徴とする請求項39記載の情報処理装置。

【請求項41】 上記第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生手段を備え、

上記制御手段は、上記プログラム更新要求に応じて、上記記録媒体を再生させるよう上記再生手段を制御し、

上記暗号化プログラムデータ受信手段は、上記再生手段で再生された上記暗号化プログラムデータを受信することを特徴とする請求項39記載の情報処理装置。

【請求項42】 上記プログラム送信手段と上記プログラム受信手段とを接続する配線を多層基板の内層に施すことを特徴とする請求項39記載の情報処理装置。

【請求項43】 上記制御部は、ボールグリッドアレイであることを特徴とする請求項39記載の情報処理装置。

【請求項44】 上記暗号化プログラムデータ受信手段で受信される暗号化プログラムデータは、上記第2のプログラムのプログラムデータから所定の演算によって算出された第1の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含むことを特徴とする請求項39記載の情報処理装置。

【請求項45】 上記復号手段は、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第1の検証データと、上記検証プログラムに復号し、上記プログラム書き込み手段は、上記復号手段で復号された上記第1の検証データと、上記検証プログラムとを上記記憶手段に書き込み、

上記制御手段は、上記第2のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記第2のプログラムのプログラムデータから第2の検証データを算出し、算出された上記第2の検証データと、上記記憶手段に記憶されている上記第1の検証データとを比較し、比較した上記第1の検証データと、上記第2の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記第2のプログラムを読み出すことを特徴とする請求項43記載の情報処理装置。

【請求項46】 第1のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第1のプログラムを読み出し、読み出した上記第1のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置のプログラム更新方法であって、

上記第1のプログラムの更新を要求するプログラム更新要求に応じて、第2のプログラムを所定の暗号化鍵で暗

号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、
 上記暗号化プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記第2のプログラムに復号する復号ステップと、
 上記復号ステップで上記暗号化プログラムデータから復号された上記第2のプログラムを上記制御部に送信するプログラム送信ステップとを備え、
 上記プログラム送信ステップによって上記制御部に送信された上記第2のプログラムを受信するプログラム受信ステップと、
 上記プログラム受信ステップで受信した上記第2のプログラムを上記記憶手段に書き込むプログラム書き込みステップとを有することを特徴とするプログラム更新方法。

【請求項47】 上記暗号化プログラムデータ受信ステップは、外部装置から送信される暗号化プログラムデータを受信することを特徴とする請求項46記載のプログラム更新方法。

【請求項48】 上記第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生ステップを備え、
 上記再生ステップは、上記プログラム更新要求を受信したことに応じて上記記録媒体を再生させ、
 上記暗号化プログラムデータ受信ステップは、上記再生ステップで再生された上記暗号化プログラムデータを受信することを特徴とする請求項46記載のプログラム更新方法。

【請求項49】 上記暗号化プログラムデータ受信ステップは、上記第2のプログラムのプログラムデータから所定の演算によって算出された第1の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含んだ上記暗号化プログラムデータを受信することを特徴とする請求項46記載のプログラム更新方法。

【請求項50】 上記復号ステップは、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第1の検証データと、上記検証プログラムに復号し、
 上記プログラム書き込みステップは、上記復号ステップで復号された上記第1の検証データと、上記検証プログラムとを上記記憶手段に書き込み、
 上記制御手段で上記第2のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記第2のプログラムのプログラムデータから第2の検証データを算出する検証データ算出ステップと、
 上記検証データ算出ステップで算出された上記第2の検証データと、上記記憶手段に記憶されている上記第1の

検証データとを比較する検証データ比較ステップと、
 上記検証データ比較ステップによって比較された上記第1の検証データと、上記第2の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記第2のプログラムを読み出すプログラム読み出しステップとを備えることを特徴とする請求項49記載のプログラム更新方法。

【請求項51】 第1のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第1のプログラムを読み出し、読み出した上記第1のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置の上記第1のプログラムを更新するためのプログラムを記録した記録媒体であって、

上記第1のプログラムの更新を要求するプログラム更新要求に応じて、第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、
 上記暗号化プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記第2のプログラムに復号する復号ステップと、
 上記復号ステップで上記暗号化プログラムデータから復号された上記第2のプログラムを上記制御部に送信するプログラム送信ステップとを備え、
 上記プログラム送信ステップによって上記制御部に送信された上記第2のプログラムを受信するプログラム受信ステップと、
 上記プログラム受信ステップで受信した上記第2のプログラムを上記記憶手段に書き込むプログラム書き込みステップとを有することを特徴とするプログラムを記録した記録媒体。

【請求項52】 上記暗号化プログラムデータ受信ステップは、外部装置から送信される暗号化プログラムデータを受信することを特徴とするプログラム記録した請求項51記載の記録媒体。

【請求項53】 上記第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生ステップを備え、
 上記再生ステップは、上記プログラム更新要求を受信したことに応じて上記記録媒体を再生させ、
 上記暗号化プログラムデータ受信ステップは、上記再生ステップで再生された上記暗号化プログラムデータを受信することを特徴とするプログラムを記録した請求項51記載の記録媒体。

【請求項54】 上記暗号化プログラムデータ受信ステップは、上記第2のプログラムのプログラムデータから所定の演算によって算出された第1の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含んだ上記暗号化プログ

ラムデータを受信することを特徴とするプログラムを記録した請求項51記載の記録媒体。

【請求項55】 上記復号ステップは、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第1の検証データと、上記検証プログラムに復号し、

上記プログラム書き込みステップは、上記復号ステップで復号された上記第1の検証データと、上記検証プログラムとを上記記憶手段に書き込み、

上記制御手段で上記第2のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記第2のプログラムのプログラムデータから第2の検証データを算出する検証データ算出ステップと、算出された上記第2の検証データと、上記記憶手段に記憶されている上記第1の検証データとを比較する検証データ比較ステップと、

上記検証データ比較ステップによって比較された上記第1の検証データと、上記第2の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記第2のプログラムを読み出すプログラム読み出しステップと備えることを特徴とするプログラムを記録した請求項54記載の記録媒体。

【請求項56】 所定のデータ処理を行うデータ処理部を備えた情報処理装置であって、

上記データ処理部は、

所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、

上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号手段と、

上記復号手段で上記暗号化プログラムデータから復号された上記所定のプログラムを記憶する記憶手段と、

上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出し手段と、

上記プログラム読み出し手段によって読み出された上記所定のプログラムに基づいて、当該データ処理部における所定のデータ処理動作を制御する第1の制御手段と、

上記復号手段で復号された上記所定のプログラム及び上記記憶手段に記憶された上記所定のプログラムの外部装置からの取り出しを制限する取り出し制限手段とを有することを特徴とする情報処理装置。

【請求項57】 上記暗号化プログラムデータが記憶された暗号化プログラムデータ記憶手段を備え、

上記第1の制御手段は、上記暗号化プログラムデータ記憶手段に記憶されている上記暗号化プログラムデータを読み出し、

上記暗号化プログラムデータ受信手段は、上記第1の制御手段によって読み出された上記暗号化プログラムデー

タを受信することを特徴とする請求項56記載の情報処理装置。

【請求項58】 上記暗号化プログラムデータ記憶手段に記憶されている上記暗号化プログラムデータを読み出す第2の制御手段を備え、

上記暗号化プログラムデータ受信手段は、上記第2の制御手段によって読み出された上記暗号化プログラムデータを受信することを特徴とする請求項56記載の情報処理装置。

10 【請求項59】 上記暗号化プログラムデータ受信手段は、外部装置から送信される暗号化プログラムデータを受信することを特徴とする請求項56記載の情報処理装置。

【請求項60】 上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生手段を備え、

上記第1の制御手段は、上記記録媒体を再生させるよう上記再生手段を制御し、

上記暗号化プログラムデータ受信手段は、上記再生手段で再生された上記暗号化プログラムデータを受信することを特徴とする請求項56記載の情報処理装置。

20 【請求項61】 上記暗号化プログラムデータ受信手段で受信される暗号化プログラムデータは、上記所定のプログラムのプログラムデータから所定の演算によって算出された第1の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含むことを特徴とする請求項56記載の情報処理装置。

30 【請求項62】 上記復号手段は、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第1の検証データと、上記検証プログラムに復号し、上記記憶手段は上記復号手段で復号された上記第1の検証データと、上記検証プログラムとを記憶し、

上記第1の制御手段は、上記所定のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記所定のプログラムのプログラムデータから第2の検証データを算出し、算出された上記第2の検証データと、上記記憶手段に記憶されている上記第1の検証データとを比較し、

40 上記プログラム読み出し手段は、上記第1の制御手段によって比較された上記第1の検証データと、上記第2の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記所定のプログラムを読み出すことを特徴とする請求項61記載の情報処理装置。

【請求項63】 所定のデータ処理を行うデータ処理部を備えた情報処理装置の上記データ処理部でのプログラムロード方法であって、

50 所定のプログラムを所定の暗号化鍵で暗号化した暗号化

プログラムデータを受信する暗号化プログラムデータ受信ステップと、

上記プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号ステップと、

上記復号された上記所定のプログラムの外部装置からの取り出しを制限する取り出し制限ステップと、

上記復号ステップで上記暗号化プログラムデータから復号された上記所定のプログラムを記憶手段に記憶させる記憶ステップと、

上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出しステップと、

上記プログラム読み出しステップによって読み出された上記所定のプログラムに基づいて、当該データ処理部における所定のデータ処理動作を制御する制御ステップと有することを特徴とするプログラムロード方法。

【請求項64】 上記制御ステップは、上記暗号化プログラムデータが記憶されている当該情報処理装置に備えられた暗号化プログラムデータ記憶手段から上記暗号化プログラムデータを読み出し、

上記暗号化プログラムデータ受信ステップは、読み出された上記暗号化プログラムデータを受信することを特徴とする請求項63記載のプログラムロード方法。

【請求項65】 上記暗号化プログラムデータ受信ステップは、外部装置から送信される暗号化プログラムデータを受信することを特徴とする請求項63記載のプログラムロード方法。

【請求項66】 上記所定のプログラムを上記の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生ステップを備え、

上記暗号化プログラムデータ受信ステップは、上記再生ステップで再生された上記暗号化プログラムデータを受信することを特徴とする請求項63記載のプログラムロード方法。

【請求項67】 上記暗号化プログラムデータ受信ステップは、上記所定のプログラムのプログラムデータから所定の演算によって算出された第1の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含んだ上記暗号化プログラムデータを受信することを特徴とする請求項63記載のプログラムロード方法。

【請求項68】 上記復号ステップは、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第1の検証データと、上記検証プログラムに復号し、

上記記憶ステップは、上記記憶手段に上記復号ステップで復号された上記第1の検証データと、上記検証プログラムとを記憶し、

上記制御ステップで、上記所定のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記所定のプログラムのプログラムデータから第2の検証データを算出する検証データ算出ステップと、

上記検証データ算出ステップによって算出された上記第2の検証データと、上記記憶手段に記憶されている上記第1の検証データとを比較する検証データ比較ステップとを備え、

10 上記プログラム読み出しステップは、上記検証データ比較ステップによって比較された上記第1の検証データと、上記第2の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記所定のプログラムを読み出すことを特徴とする請求項67記載のプログラムロード方法。

【請求項69】 所定のデータ処理を行うデータ処理部を備えた情報処理装置の上記データ処理部で所定のプログラムをロードするためのプログラムを記録した記録媒体であって、

20 上記所定のプログラムを上記の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、

上記プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号ステップと、

上記復号された上記所定のプログラムの外部装置からの取り出しを制限する取り出し制限ステップと、

上記復号ステップで上記暗号化プログラムデータから復号された上記所定のプログラムを記憶手段に記憶する記憶ステップと、

30 上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出しステップと、

上記プログラム読み出しステップによって読み出された上記所定のプログラムに基づいて、上記データ処理部における所定のデータ処理動作を制御する制御ステップと有することを特徴とするプログラムが記録された記録媒体。

【請求項70】 上記制御ステップは、上記暗号化プログラムデータが記憶されている当該情報処理装置に備えられた暗号化プログラムデータ記憶手段に記憶されている上記暗号化プログラムデータを読み出し、

40 上記暗号化プログラムデータ受信ステップは、上記制御ステップによって読み出された上記暗号化プログラムデータを受信することを特徴とするプログラムが記録された請求項69記載の記録媒体。

【請求項71】 上記暗号化プログラムデータ受信ステップは、外部装置から送信される暗号化プログラムデータを受信することを特徴とするプログラムが記録された請求項69記載の記録媒体。

【請求項72】 上記所定のプログラムを上記の暗号化

50 上記所定のプログラムを上記の暗号化

鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生ステップを備え、

上記暗号化プログラムデータ受信ステップは、上記再生ステップで再生された上記暗号化プログラムデータを受信することを特徴とするプログラムが記録された請求項69記載の記録媒体。

【請求項73】 上記暗号化プログラムデータ受信ステップは、上記所定のプログラムのプログラムデータから所定の演算によって算出された第1の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含んだ上記暗号化プログラムデータを受信することを特徴とするプログラムを記録した請求項69記載の記録媒体。

【請求項74】 上記復号ステップは、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第1の検証データと、上記検証プログラムに復号し、

上記記憶ステップは、上記記憶手段に上記復号ステップで復号された上記第1の検証データと、上記検証プログラムとを記憶し、

上記制御ステップで、上記所定のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記所定のプログラムのプログラムデータから第2の検証データを算出する検証データ算出ステップと、

上記検証データ算出ステップで算出された上記第2の検証データと、上記記憶手段に記憶されている上記第1の検証データとを比較する検証データ比較ステップとを備え、

上記プログラム読み出しステップは、上記検証データ比較ステップによって比較された上記第1の検証データと、上記第2の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記所定のプログラムを読み出すことを特徴とするプログラムを記録した請求項73記載の記録媒体。

【請求項75】 情報処理装置の所定のデータ処理を行うデータ処理手段を集積化した回路素子であって、所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、

上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号手段と、

上記復号手段で上記暗号化プログラムデータから復号された上記所定のプログラムを記憶する記憶手段と、

上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出し手段と、

上記プログラム読み出し手段によって読み出された上記

所定のプログラムに基づいて、上記データ処理手段における所定のデータ処理動作を制御する第1の制御手段と、

上記復号手段で復号された上記所定のプログラム及び上記記憶手段に記憶された上記所定のプログラムの外部装置からの取り出しを制限する取り出し制限手段とを集積化してなることを特徴とする回路素子。

【請求項76】 上記暗号化プログラムデータが記憶された暗号化プログラムデータ記憶手段を有する情報処理装置に備えられ、

上記第1の制御手段は、上記暗号化プログラムデータ記憶手段に記憶されている上記暗号化プログラムデータを読み出し、

上記暗号化プログラムデータ受信手段は、上記第1の制御手段によって読み出された上記暗号化プログラムデータを受信することを特徴とする請求項75記載の回路素子。

【請求項77】 第2の制御手段を有する上記情報処理装置に備えられ、

上記第2の制御手段は、上記暗号化プログラムデータ記憶手段に記憶されている上記暗号化プログラムデータを読み出し、

上記暗号化プログラムデータ受信手段は、上記第2の制御手段によって読み出された上記暗号化プログラムデータを受信することを特徴とする請求項75記載の回路素子。

【請求項78】 上記暗号化プログラムデータ受信手段は、外部装置から送信される暗号化プログラムデータを受信することを特徴とする請求項75記載の回路素子。

【請求項79】 上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータが記録された記録媒体を再生する再生手段を有する情報処理装置に備えられ、

上記第1の制御手段は、上記記録媒体を再生させるよう上記再生手段を制御し、

上記暗号化プログラムデータ受信手段は、上記再生手段で再生された上記暗号化プログラムデータを受信することを特徴とする請求項75記載の回路素子。

【請求項80】 上記暗号化プログラムデータ受信手段で受信される暗号化プログラムデータは、上記所定のプログラムのプログラムデータから所定の演算によって算出された第1の検証データと、上記所定の演算をするプログラムである検証プログラムとが上記所定の暗号化鍵で暗号化された暗号化検証データと、暗号化検証プログラムとを含むことを特徴とする請求項75記載の回路素子。

【請求項81】 上記復号手段は、上記暗号化プログラムデータを復号する際、上記暗号化検証データと、上記暗号化検証プログラムとを上記所定の復号鍵を用いて上記第1の検証データと、上記検証プログラムに復号し、

上記記憶手段は上記復号手段で復号された上記第1の検証データと、上記検証プログラムとを記憶し、

上記第1の制御手段は、上記所定のプログラムを実行する前に、上記検証プログラムに基づいて、上記記憶手段に記憶された上記所定のプログラムのプログラムデータから第2の検証データを算出し、算出された上記第2の検証データと、上記記憶手段に記憶されている上記第1の検証データとを比較し、

上記プログラム読み出し手段は、上記第1の制御手段によって比較された上記第1の検証データと、上記第2の検証データとが一致したことに応じて、上記記憶手段に記憶されている上記所定のプログラムを読み出すことを特徴とする請求項80記載の回路素子。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理装置のプログラム更新に関するものであり、詳しくはプログラムの更新、又は、プログラムのロード時に、プログラムデータの漏洩を阻止することでプログラムが改竄されることを防止する情報処理装置、プログラムロード方法、記録媒体、プログラム更新方法及び回路素子に関する。

【0002】

【従来の技術】DVD (Digital Versatile Disc) は、映画1本分相当の映像と音声のデジタルデータを記録できる記録容量を持つ光ディスクであり、ROM (DVD-ROM: DVD-Read Only Memory) として利用されている。

【0003】DVD-ROMは劣化のないデジタルデータを記録しているため、記憶されているデジタルデータの違法コピーや、違法利用を防止するためにいくつかのプロテクト機能が備えられている。

【0004】例えば、DVD-ROMを再生する際のプロテクト機能としては、リージョナルコード (RC: Regional Code) による再生制限がある。リージョナルコードとは、世界を6つに分けて、それぞれに付与した番号のことである。例えば、アメリカのリージョナルコードは"1"であり、日本のリージョナルコードは"2"である。

【0005】リージョナルコードは、DVD-ROMとDVD-ROMを再生するDVD-ROMドライブ又はDVD再生アプリケーションにそれぞれ与えられ、それぞれのリージョナルコードが一致しないと、再生をすることができないようになっている。例えば、日本で生産されたDVD-ROMドライブにはリージョナルコード"2"が与えられているため、アメリカで生産されたリージョナルコード"1"のDVD-ROMを再生することはできない。これは、映画などのコンテンツ制作者を保護する目的で付けられたプロテクト機能である。

【0006】また、DVD-ROMには、デジタルコピーを防止するプロテクト機能がある。これは、CSS (Content Scrambling System) と呼ばれており、ファ

イル自体は、ハードディスクなどにコピー可能であるが、コピーしたファイルを再生させると暗号化されたデータであるため、MPEG (Moving Picture Experts Group) データのデコードをできないようにさせることでデジタルコピーを防止している。

【0007】他に、DVD-ROMには、アナログ出力されたデータのコピーを防止するプロテクト機能や、デジタル機器間でのデジタルデータのコピー世代を管理し制限するプロテクト機能などがある。

10 【0008】このようなプロテクト機能は、DVD-ROMドライブ内の所定のROMに書き込まれたファームウェアと呼ばれるプログラムによって実行される。ファームウェアは、ハードウェアを直接的に制御するソフトウェアをROMに書き込み、ハードウェア内に組み込んだものである。

【0009】DVD-ROMドライブの所定のROMに書き込まれたプロテクト機能を実行するファームウェアによって、不正に作成されたDVD-Videoを排除することができる。

20 【0010】ところで、一般に、このようなファームウェアを書き換えたり変更することは困難であるが、例えば、PC (Personal Computer) などに接続し、PCの制御によって作動するDVD-ROMドライブなどでは、PCのOS (Operating System) がアップデートされることに伴ってファームウェアもアップデートする必要が生じてくる。したがって、このような、DVD-ROMではファームウェアの更新を可能とするような構成となっている。

30 【0011】また、PCと、DVD-ROMドライブとの接続の相性がよくない場合なども、DVD-ROMドライブのファームウェアを更新することで改善させることができる。

【0012】ファームウェアを更新可能とするには、当該ファームウェアを格納するROMにデータの電気的消去が可能なプログラマブルROMであるEEPROM (Electrically Erasable Programmable Read-Only Memory) などの、いわゆるフラッシュメモリが用いられる。

【0013】

40 【発明が解決しようとする課題】しかし、このようなファームウェアを更新する場合、ファームウェアをDVD-ROMドライブのメーカーが提供するホームページなどからインターネットで簡単にダウンロードできるため、ユーザはファームウェアを簡単に入手することができる。

【0014】さらに、ユーザは入手したファームウェアを改竄し、DVD-ROMドライブの所定のフラッシュメモリに格納することで、上述したDVD-ROMのプロテクト機能を無効化させるといった問題がある。

50 【0015】上述したファームウェアに限らずプログラ

ムの改竄は、プログラムの転送を必要とする装置には必ず生ずる問題である。改竄プログラムを使用した装置は、期待される動作と異なる動作をしたり、さらに最悪の場合には故障をしてしまうといった問題をも含んでいる。

【0016】そこで、本発明は上述したような問題を解決するために案出されたものであり、プログラムの更新、又は、プログラムのロード時に、外部にプログラムデータが漏洩することによって生ずるプログラムの改竄を阻止し、デジタルデータの不正利用を防止する情報処理装置、プログラムロード方法、記録媒体、プログラム更新方法及び回路素子を提供することを目的とする。

【0017】

【課題を解決するための手段】上述の目的を達成するために、本発明に係る情報処理装置は、所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号手段と、上記復号手段で上記暗号化プログラムデータから復号された上記所定のプログラムを記憶する記憶手段と、上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出し手段と、上記読み出し手段によって読み出された上記所定のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを備えることを特徴とする。

【0018】上述の目的を達成するために、本発明に係るプログラムロード方法は、情報処理装置に所定のプログラムをロードするためのプログラムロード方法であって、上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、上記暗号化プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号ステップと、上記復号ステップで上記暗号化プログラムデータから復号された上記所定のプログラムを記憶手段に記憶する記憶ステップと、上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出しステップと、上記読み出しステップによって読み出された上記所定のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御ステップとを備えることを特徴とする。

【0019】上述の目的を達成するために、本発明に係る記録媒体は、情報処理装置に所定のプログラムをロードするためのプログラムを記録した記録媒体であって、上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、上記暗号化プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号ス

テップと、上記復号ステップで上記暗号化プログラムデータから復号された上記所定のプログラムを記憶手段に記憶する記憶ステップと、上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出しステップと、上記読み出しステップによって読み出された上記所定のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御ステップとを備えることを特徴とするプログラムが記録されている。

【0020】上述の目的を達成するために、本発明に係る情報処理装置は、第1のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第1のプログラムを読み出し、読み出した上記第1のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置であって、上記制御部は、上記第1のプログラムの更新を要求するプログラム更新要求に応じて、第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記第2のプログラムに復号する復号手段と、上記復号手段で上記暗号化プログラムデータから復号された第2のプログラムを、上記記憶手段に書き込むプログラム書き込み手段と、上記復号手段で復号された第2のプログラム及び上記記憶手段に書き込まれた第2のプログラムの外部装置からの取り出しを制限する取り出し制限手段とを備えることを特徴とする。

【0021】上述の目的を達成するために、本発明に係るプログラム更新方法は、第1のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第1のプログラムを読み出し、読み出した上記第1のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置のプログラム更新方法であって、上記第1のプログラムの更新を要求するプログラム更新要求に応じて、第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、上記受信した暗号化プログラムデータを所定の復号鍵を用いて上記第2のプログラムに復号する復号ステップと、上記復号された第2のプログラムの外部装置からの取り出しを制限する取り出し制限ステップと、上記暗号化プログラムデータから復号された第2のプログラムを、上記記憶手段に書き込むプログラム書き込みステップとを備えることを特徴とする。

【0022】上述の目的を達成するために、本発明に係る記録媒体は、第1のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第1のプログラムを読み出し、読み出した上記第1のプログラムに基づいて所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置の上記第1のプログラムを更新する

ためのプログラムを記録した記録媒体であって、上記第 1 のプログラムの更新を要求するプログラム更新要求に応じて、第 2 のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、上記受信した暗号化プログラムデータを所定の復号鍵を用いて上記第 2 のプログラムに復号する復号ステップと、上記復号された第 2 のプログラムの外部装置からの取り出しを制限する取り出し制限ステップと、上記暗号化プログラムデータから復号された第 2 のプログラムを上記記憶手段に書き込むプログラム書き込みステップとを備えることを特徴とするプログラムが記録されている。

【0023】 上述の目的を達成するために、本発明に係る回路素子は、第 1 のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第 1 のプログラムを読み出し、読み出した上記第 1 のプログラムに基づいて情報処理装置の所定の動作を制御する制御手段とを集積化した回路素子であって、上記第 1 のプログラムの更新を要求するプログラム更新要求に応じて、第 2 のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記第 2 のプログラムに復号する復号手段と、上記復号手段で上記暗号化プログラムデータから復号された第 2 のプログラムを、上記記憶手段に書き込むプログラム書き込み手段と、上記復号手段で復号された第 2 のプログラム及び上記記憶手段に書き込まれた第 2 のプログラムの外部装置からの取り出しを制限する取り出し制限手段とを集積化してなることを特徴とする。

【0024】 上述の目的を達成するために、本発明に係る情報処理装置は、第 1 のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第 1 のプログラムを読み出し、読み出した上記第 1 のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置であって、上記第 1 のプログラムの更新を要求するプログラム更新要求に応じて、第 2 のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記第 2 のプログラムに復号する復号手段と、上記復号手段で上記暗号化プログラムデータから復号された上記第 2 のプログラムを上記制御部に送信するプログラム送信手段とを備え、上記制御部は、上記送信手段によって送信された上記第 2 のプログラムを受信するプログラム受信手段と、上記プログラム受信手段で受信した上記第 2 のプログラムを上記記憶手段に書き込むプログラム書き込み手段とを有することを特徴とする。

【0025】 上述の目的を達成するために、本発明に係るプログラム更新方法は、第 1 のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第 1 のプログラムを読み出し、読み出した上記第 1 のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置のプログラム更新方法であって、上記第 1 のプログラムの更新を要求するプログラム更新要求に応じて、第 2 のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、上記暗号化プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記第 2 のプログラムに復号する復号ステップと、上記復号ステップで上記暗号化プログラムデータから復号された上記第 2 のプログラムを上記制御部に送信するプログラム送信ステップとを備え、上記プログラム送信ステップによって上記制御部に送信された上記第 2 のプログラムを受信するプログラム受信ステップと、上記プログラム受信ステップで受信した上記第 2 のプログラムを上記記憶手段に書き込むプログラム書き込みステップとを有することを特徴とする。

【0026】 上述の目的を達成するために、本発明に係る記録媒体は、第 1 のプログラムが記憶された記憶手段と、上記記憶手段に記憶されている上記第 1 のプログラムを読み出し、読み出した上記第 1 のプログラムに基づいて当該情報処理装置の所定の動作を制御する制御手段とを有する制御部を備えた情報処理装置の上記第 1 のプログラムを更新するためのプログラムを記録した記録媒体であって、上記第 1 のプログラムの更新を要求するプログラム更新要求に応じて、第 2 のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、上記暗号化プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記第 2 のプログラムに復号する復号ステップと、上記復号ステップで上記暗号化プログラムデータから復号された上記第 2 のプログラムを上記制御部に送信するプログラム送信ステップとを備え、上記プログラム送信ステップによって上記制御部に送信された上記第 2 のプログラムを受信するプログラム受信ステップと、上記プログラム受信ステップで受信した上記第 2 のプログラムを上記記憶手段に書き込むプログラム書き込みステップとを有することを特徴とするプログラムが記録されている。

【0027】 上述の目的を達成するために、本発明に係る情報処理装置は、所定のデータ処理を行うデータ処理部を備えた情報処理装置であって、上記データ処理部は、所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を

用いて上記所定のプログラムに復号する復号手段と、上記復号手段で上記暗号化プログラムデータから復号された上記所定のプログラムを記憶する記憶手段と、上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出し手段と、上記プログラム読み出し手段によって読み出された上記所定のプログラムに基づいて、当該データ処理部における所定のデータ処理動作を制御する第1の制御手段と、上記復号手段で復号された上記所定のプログラム及び上記記憶手段に記憶された上記所定のプログラムの外部装置からの取り出しを制限する取り出し制限手段とを有することを特徴とする。

【0028】上述の目的を達成するために、本発明に係るプログラムロード方法は、所定のデータ処理を行うデータ処理部を備えた情報処理装置の上記データ処理部でのプログラムロード方法であって、所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、上記プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号ステップと、上記復号された上記所定のプログラムの外部装置からの取り出しを制限する取り出し制限ステップと、上記復号ステップで上記暗号化プログラムデータから復号された上記所定のプログラムを記憶手段に記憶させる記憶ステップと、上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出しステップと、上記プログラム読み出しステップによって読み出された上記所定のプログラムに基づいて、当該データ処理部における所定のデータ処理動作を制御する制御ステップとを有することを特徴とする。

【0029】上述の目的を達成するために、本発明に係る記録媒体は、所定のデータ処理を行うデータ処理部を備えた情報処理装置の上記データ処理部で所定のプログラムをロードするためのプログラムを記録した記録媒体であって、上記所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信ステップと、上記プログラムデータ受信ステップで受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号ステップと、上記復号された上記所定のプログラムの外部装置からの取り出しを制限する取り出し制限ステップと、上記復号ステップで上記暗号化プログラムデータから復号された上記所定のプログラムを記憶手段に記憶する記憶ステップと、上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出しステップと、上記プログラム読み出しステップによって読み出された上記所定のプログラムに基づいて、上記データ処理部における所定のデータ処理動作を制御する制御ステップとを有することを特徴とするプログラムが記録されている。

【0030】上述の目的を達成するために、本発明に係

る回路素子は、情報処理装置の所定のデータ処理を行うデータ処理手段を集積化した回路素子であって、所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを受信する暗号化プログラムデータ受信手段と、上記暗号化プログラムデータ受信手段で受信した上記暗号化プログラムデータを所定の復号鍵を用いて上記所定のプログラムに復号する復号手段と、上記復号手段で上記暗号化プログラムデータから復号された上記所定のプログラムを記憶する記憶手段と、上記記憶手段に記憶された上記所定のプログラムを読み出すプログラム読み出し手段と、上記プログラム読み出し手段によって読み出された上記所定のプログラムに基づいて、上記データ処理手段における所定のデータ処理動作を制御する第1の制御手段と、上記復号手段で復号された上記所定のプログラム及び上記記憶手段に記憶された上記所定のプログラムの外部装置からの取り出しを制限する取り出し制限手段とを集積化して有することを特徴とする。

【0031】

【発明の実施の形態】以下、本発明に係る情報処理装置、プログラムロード方法、記録媒体、プログラム更新方法及び回路素子の実施の形態を図面を参照にして詳細に説明する。

【0032】まず、図1に第1の実施の形態として示すDVD-ROMドライブの構成について説明をする。

【0033】DVD-ROMドライブは、DVD-ROM (Digital Versatile Disc-Read Only Memory) 1を所定の箇所に装着し、装着したDVD-ROM 1を再生する装置である。DVD-ROMドライブは、PC (Personal Computer) 10に接続され、装着したDVD-ROM 1の再生動作などの各種動作は、接続されたPC 10によって制御される。

【0034】DVD-ROMドライブは、光学ピックアップユニット2と、スピンドルモータ3と、リードプロセッサ4と、光学ピックアップユニットドライバ5と、スピンドルモータドライバ6と、DVDデコーダ7と、バッファメモリ8と、CPU9とを備える。

【0035】光学ピックアップユニット2は、図示しないが、所定の波長のレーザ光を出射するレーザダイオードと、レーザダイオードから出射された所定の波長のレーザ光をDVD-ROM 1のデータ記録面に集光して出射し、DVD-ROM 1のデータ記録面で反射された反射光を集光して出射する対物レンズと、所定の制御信号に応じて上記対物レンズを搭載し対物レンズを駆動させフォーカス調整及びトラッキング調整を行う2軸アクチュエータと、DVD-ROM 1のデータ記録面で反射された反射光を受光し電気信号に変換することでデータ記録面のピットの有無を検出するフォトディテクタとを備えている。フォトディテクタで検出された電気信号は、一般にRF (Radio Frequency) 信号と呼ばれている。

【0036】また、当該光学ピックアップユニット2に

は、当該光学ピックアップユニット2をDVD-ROM 1の半径方向に駆動させるスレッドモータが備えられている。

【0037】さらにまた、当該DVD-ROMドライブが、図示しないディスクトレイにDVD-ROM1を載せてローディングする機構を備えている場合は、このディスクトレイを動作させるローディングモータもこの光学ピックアップユニット2に備えられていてもよい。

【0038】スピンドルモータ3は、装着されたDVD-ROM1を回転駆動させるモータである。

【0039】リードプロセッサ4は、光学ピックアップユニット2が備えるフォトディテクタで検出されたRF信号からDVD読み出し用EFM+ (Eight to Fourteen Plus Modulation) 信号と、フォーカサー用のFE (Focus Error) 信号、トラッキングサーボ用のTE (Tracking Error) 信号、Pull-in信号を生成し、後述するDVDデコーダ7のサーボ制御部12に送出する。

【0040】光学ピックアップユニットドライバ5は、所定の制御信号に応じて上述の光学ピックアップユニット2の図示しない2軸アクチュエータ、スレッドモータ、ローディングモータをそれぞれ駆動させるドライバIC (Integrated Circuit) である。

【0041】スピンドルモータドライバ6は、所定の制御信号に応じて上述のスピンドルモータ3を駆動させるドライバICである。

【0042】DVDデコーダ7は、DVD信号処理部11と、サーボ制御部12と、ディスク回転制御部13と、メモリ制御部14と、ATAPI (AT Attachment with Packet Interface) 15と、CPU 1/F16とを備えている。

【0043】DVD信号処理部11は、RS-PC復号器、アドレス検出のためのID処理、8/16変換回路、記録可能メディアか否かを判定するためのWobbleディテクタを備えている。

【0044】サーボ制御部12は、リードプロセッサ4から送信されたFE信号、TE信号、Pull-in信号に応じて、光学ピックアップユニット2の2軸アクチュエータ、スレッドモータを駆動制御するための制御信号を生成し、光学ピックアップユニットドライバ5へ送出する。

【0045】ディスク回転制御部13は、DVD-ROM1を装着したスピンドルモータ3の回転を制御する制御信号を生成し、スピンドルモータドライバ6へ送出する。

【0046】メモリ制御部14は、バッファメモリ8へデータの書き込み、読み出しを制御する。

【0047】ATAPI 15は、PC10と、当該DVD-ROMドライブとを接続し、データのやり取りを行うためのインターフェースである。

【0048】なお、PC10と接続するためのインターフェースは、このATAPI 15以外にも、例えば、SCSI (Small Computer System Interface)、USB (Universal Serial Bus)、IEEE (Institute of Electrical and Electronics Engineers) 1394などであってもよい。

【0049】CPU 1/F16は、当該DVDデコーダ7とCPU9とを接続し、CPU9から当該DVDデコーダ7を制御するためのインターフェースである。また、CPU 1/F16は、バッファメモリ8に記憶されているデータを読み出したり、バッファメモリ8にデータを書き込んだりする。

【0050】バッファメモリ8は、例えば、DRAM (Dynamic Random-Access Memory) などのランダムアクセス可能なメモリであり、DVD信号処理部11から送出されたデータ、PC10から送出されたデータ、CPU9から送出されたデータを一時的に記憶する。

【0051】CPU9は、CPU 1/F16でDVDデコーダ7と接続され、DVD-ROMドライブの各機能を統括的に制御する。CPU9の構成及び機能については、後で詳細に説明をする。

【0052】PC10は、DVD-ROMドライブと、DVDデコーダ7のATAPI 15などで接続され、DVD-ROMドライブの動作、例えば、再生、停止、データ検索などを、所定のコマンドを入力することで制御する。ユーザは、PC10を介して、DVD-ROM1の各種データを利用することができる。

【0053】続いて、CPU9の構成について詳細に説明をする。

【0054】CPU9は、CPUコア20と、ブートROM21と、フラッシュROM22と、RAM23と、入力/出力ポート24と、書き込みタイミング制御用タイマー25と、割り込み制御回路26と、シリアル通信回路27と、32bitバス28、16bitバス29と、ブリッジ回路30と、外部バスコントローラ31とを備えている。

【0055】CPUコア20は、CPU9における中心部分で四則演算や比較判断をする論理演算装置や加算回路、レジスタなどを備えている。

【0056】ブートROM21は、例えば、データの電氣的消去が可能なプログラマブルROMであるEEPROM (Electrically Erasable Programmable Read-Only Memory) などのいわゆるフラッシュメモリである。

【0057】ブートROM21には、フラッシュROM22に記憶されたプログラムをアップデートする際に起動させるブートプログラムを格納している。このブートプログラムを起動させるには、例えば、CPU9に設けられた端子に所定の電圧を印加することで実行する。上述の端子に所定の電圧が印加されると、ブートプログラムが先頭アドレスから読み出されブートプログラムが実

行される。

【0058】またブートROM21は、暗号化され送信されたファームウェアを解読するために用いる共通鍵をプログラムとして格納すると共に、この共通鍵を用いて暗号化されたファームウェアを解読する暗号解読アルゴリズムを格納した暗号化処理部21aを備えている。

【0059】フラッシュROM22は、ブートROM21と同様に、例えば、データの電氣的消去が可能なプログラマブルROMであるEEPROMなどのいわゆるフラッシュメモリである。

【0060】フラッシュROM22には、ファームウェアが格納され、当該DVD-ROMドライブの再生制限をするプログラムであるファームウェアが格納される。フラッシュROM22に格納されたファームウェアは、DVD-ROMドライブの所定の動作、例えば、DVD-ROM1の再生制限や、デジタルコピーの制限をするプログラムである。

【0061】また、フラッシュROM22に代えてTMR (Tunneling Magneto Resistive) 素子を用いたMRAM (Magnetic Random Access Memory) を使用してもよい。MRAMは、磁気によってデータを記憶するメモリであるためデータのオーバーライトが可能である。したがって、ファームウェアを更新する際に、MRAMに記憶されているデータ、つまり更新前のファームウェアの消去動作が不要となる。

【0062】ここで、図2を用いて、共通鍵について説明をする。

【0063】図2に示すように、例えば、平文データを暗号化する際は所定の暗号化鍵を用いて暗号化データに変換し、再び暗号化データを復号する際は所定の復号鍵を用いて平文データとする。

【0064】言い換えると、暗号化鍵は、平文データや情報を暗号化する時に用いられ、復号鍵は、暗号化されたデータや情報をもとの平文データや情報に戻す時に用いられる。

【0065】共通鍵とは、上述のようにデータを暗号化する際に用いる暗号化鍵と、暗号化されたデータを復号する際に用いる復号鍵とが共通である鍵のことである。この共通鍵の情報は、公開されず秘密にしておくことから秘密鍵とも呼ばれている。

【0066】なお、ブートROM21及びフラッシュROM22は2つの異なるフラッシュROMを用いるように記載しているが、これを1つのフラッシュROMとし、このフラッシュROMの記憶領域をブート領域、プログラム領域のように分割するようにしてもよい。

【0067】RAM23は、記憶内容維持のためのリフレッシュ動作が不要で高速アクセス可能なSRAM (Static Random Access Memory) などであり、フラッシュROM22に格納されているファームウェアをアップデートする際にデータ及びアップデート用プログラムの展

開領域となる。

【0068】一般にフラッシュメモリでは、当該フラッシュメモリに記憶されているデータをアップデートする際、自分自身でプログラムを実行することができない。したがって、ファームウェアのアップデート時には、バッファメモリ8から転送されるファームウェアのデータと共にアップデート用のアップデート関数がブートROM21からRAM23にコピーされる。

【0069】入力/出力ポート24は、当該CPU9にデータの出力ポート、及び、当該CPU9から出力するデータの出力ポートである。

【0070】書き込みタイミング制御用タイマー25は、フラッシュROM22のファームウェアをアップデートする際の書き込みのタイミングを制御する。

【0071】割り込み制御回路26は、所定の割り込み発生に応じて現在実行中の処理を中断し割り込みプログラムを実行させるよう制御する回路である。

【0072】シリアル通信回路27は、シリアルデータを送受信するインターフェースである。

【0073】32bitバス28は、一度に32bitのデータを伝送可能なバスである。

【0074】16bitバス29は、一度に16bitのデータを伝送可能なバスである。

【0075】ブリッジ回路30は、32bitバス28と、16bitバス29とを接続する回路である。

【0076】外部バスコントローラ31は、当該CPU9と外部装置であるDVDデコーダ7との間で伝送されるデータを監視し、DVDデコーダ7とのデータ入出力を制御をする。また、外部バスコントローラ31は、当該CPU9内のブートROM21及びフラッシュROM22に格納されているプログラムとRAM23をユーザレベルでは参照できないような保護機能を備えている。これにより、共通鍵、暗号化処理部21a及び復号されたファームウェアをCPU9から取り出すことを制限することができる。

【0077】続いて、図3に示すフローチャートを用いて、フラッシュROM22に記憶されたファームウェアをアップデートする際の動作について説明をする。

【0078】まず、ステップS1において、CPU9のCPUコア20は、ブート端子にかけられた電圧がHIGHレベル (High Level) であった場合、工程をステップS2へと進め、LOWレベル (Low Level) であった場合、工程をステップS4へと進める。

【0079】ステップS2からの工程はフラッシュROM22に記憶されているプログラムを実行する工程であり、ステップS4からの工程はブートROM21に記憶されているブートプログラムを起動させ、ファームウェアをアップデートする工程である。

【0080】ステップS2において、CPUコア20は、フラッシュROM22のプログラム、例えば、ファ

ームウェアなどが記録されているプログラム領域の先頭アドレスへアクセスする。

【0081】ステップS3において、CPUコア20はアクセスしたフラッシュROM22のプログラム領域に記憶されているプログラムに応じて、DVD-ROM1に対して通常処理、例えば、再生処理、データ検索処理などを実行する。

【0082】ステップS4において、ブート端子にLOWレベルの電圧がかかったことに応じて、ブートROM21のブートプログラムが記憶されているブート領域の先頭アドレスがCPUコア20に読み込まれ、ブートプログラムが起動する。

【0083】ステップS5において、CPUコア20は、当該DVD-ROMドライブの全ポートを初期化する。これによりDVD-ROMドライブのメカ系及び電気系の破壊が防止される。

【0084】ステップS6において、CPUコア20は、PC10からNot Ready状態で実行可能なコマンドが入力されたかどうかを判断する。ここでいうNot Ready状態とは、当該DVD-ROMドライブにDVD-ROM1が装着されていない、或いはDVD-ROM1がCPU9に認識されていない状態を示し、Not Ready状態で実行可能なコマンドとは、DVD-ROM1が認識されていないくても実行可能なコマンドである。例えば、DVD-ROM1から所定のデータを読み出せというようなコマンドは、Not Readyでは実行不可能なコマンドである。

【0085】Not Ready状態で実行可能なコマンドが入力された場合は工程をステップS8へと進め、実行不可能なコマンドが入力された場合は工程をステップS7へと進める。

【0086】ステップS7において、CPUコア20は、Not Ready状態で実行不可能なコマンドが入力されたことに応じて、Check Condition Statusでコマンドを完了させ、工程を再びステップS6へと戻す。

【0087】ステップS8において、CPUコア20は、フラッシュROM22のプログラム更新を指示するWriteバッファコマンド(Write Buffer Command)とは異なるコマンドがPC10から送信された場合は工程をステップS9へと進め、Writeバッファコマンドが送信された場合は工程をステップS10へと進める。

【0088】ステップS9において、CPUコア20は、Writeバッファコマンドとは異なるコマンドが入力されたことに応じて、入力されたコマンドを実行する。

【0089】PC10は、DVD-ROMドライブにWriteバッファコマンドを送信した後、アップデートするファームウェアを共通鍵で暗号化したファームウェア

ア暗号化データをバイナリファイルとしてDVD-ROMドライブに送信する。

【0090】ステップS10において、CPUコア20は、Writeバッファコマンドを受信したことに応じて、バッファメモリ8のデータ記憶領域の所定のアドレスNから2×M(Mは自然数)KB分の領域を確保し、PC10から送信されるバイナリファイルを上記確保したデータ記憶領域に記憶させる。

【0091】CPUコア20はバイナリファイルを受信すると、全バイナリデータを加算してCheck Sumデータを生成し、バイナリファイルと共にバッファメモリ8に記憶させる。Check Sumデータは、送られてきたプログラムがエラーなく受信されたことを確認するためのデータで、送信された全てのデータを加算することで得られる。

【0092】ステップS11において、CPUコア20は、ステップS10でバッファメモリ8に格納したCheck Sumデータを検証し、送信されたファームウェア暗号化データが正しく受信されたかどうかを確認する。正しく受信されている場合は工程をステップS13へと進め、正しく受信されていない場合は工程をステップS12へと進める。

【0093】ステップS12において、CPUコア20は、ステップS11でのCheck Sumデータの検証結果から正しくバイナリファイルが送信されなかったことを、Check Condition Statusでコマンドを完了させることでPC10に知らせ、工程を再びステップS6へと戻す。

【0094】ステップS13において、CPUコア20は、ブートROM21に記憶されている、ファームウェアをアップデートする際に使用するアップデート(update)関数をRAM23にコピーする。

【0095】アップデート関数は、RAM23にコピーされ、RAM23に展開されることでファームウェアをフラッシュROM22にアップデートするためのアップデートプログラムとして機能する。

【0096】続いて、図4に示すフローチャートを用いてアップデート(update)関数による処理動作について説明をする。

【0097】ステップS21において、CPUコア20は、RAM23に格納されたアップデート関数の先頭アドレスにアクセスし、アップデート関数によるファームウェアのフラッシュROM22へのアップデートを開始する。

【0098】ステップS22において、CPUコア20は、割り込み制御回路26を制御して全ての割り込みプログラムの実行と、例外処理の実行を禁止する。

【0099】さらに、CPUコア20は、PC10から入力されたWriteバッファコマンドを受信したことに応じて、フラッシュROM22のファームウェア格納

領域に記憶されているデータを消去する。

【0100】なお、フラッシュROM22に代えて上述したMRAMを使用した場合、当該MRAMがデータのオーバーライトが可能のため記憶されているファームウェアの消去動作は不要となる。

【0101】ステップS23において、CPUコア20は、フラッシュROM22への書き込みタイミングを制御する書き込みタイミング制御用タイマー25を起動させる。

【0102】以下、フラッシュROM22へデータを書き込む際は、書き込みタイミング制御用タイマー25のタイミング制御に基づいて実行される。

【0103】ステップS24において、CPUコア20は、ファームウェア暗号化データのバイナリファイルが記憶されているバッファメモリ8のアドレス番号Nと、ファームウェアを記憶させるフラッシュROM22のアドレス番号0にアクセスをする。

【0104】ステップS25において、CPUコア20は、バッファメモリ8のアドレス番号Nから2KB分のアドレス番号までのデータを読み出しRAM23にコピーする。

【0105】ステップS26において、CPUコア20は、RAM23内にコピーされた2KB分のデータを8Byteごと読み出し、ブートROM21内の共通鍵と、暗号化処理部21aに記憶されている暗号解読アルゴリズムとで復号する。CPUコア20は、復号した2KB分のデータ、つまり暗号解読されたファームウェアデータを再びRAM23内に記憶させ展開する。

【0106】ステップS27において、CPUコア20は、RAM23内に記憶された2KBのファームウェアデータをRAM23から読み出し、フラッシュROM22のアドレス番号0から書き込む。

【0107】ステップS28において、CPUコア20は、フラッシュROM22に記憶させたファームウェアデータの最終アドレス番号が、 $2 \times M$ (M は自然数) となった場合工程をステップS30へと進め、そうでない場合は工程をステップS29へと進める。

【0108】ステップS29において、CPUコア20は、バッファメモリ8のアドレス番号及びフラッシュROM22のアドレス番号を2KB増やしたアドレス番号へアクセスをする。この工程が終了するとステップS25へと戻る。

【0109】ステップS30において、CPUコア20は、フラッシュROM22への書き込みタイミングを制御する書き込みタイミング制御用タイマー25を停止させる。

【0110】ステップS31において、ステップS28で、フラッシュROM22に記憶されたファームウェアデータの最終アドレス番号が $2 \times M$ (M は自然数) であると判定され、ステップS30で書き込みタイミング制

御用タイマー25が停止されたことで、ファームウェアのフラッシュROM22へのアップデートが完了する。

【0111】ステップS32において、ステップS31でファームウェアのアップデートが完了したことに応じて、CPUコア20は、フラッシュROM22のプログラム領域の先頭アドレスへアクセスをする。

【0112】ステップS33において、CPUコア20はアクセスしたフラッシュROM22のプログラム領域に記憶されているプログラム、つまり、更新された後のファームウェアに応じて、DVD-ROM1に対して通常処理、例えば、再生処理、データ検索処理などを実行する。

【0113】このようにして、本発明を適用したDVD-ROMドライブでは、フラッシュROM22に格納されているファームウェアをアップデートする際、PC10から共通鍵を用いて暗号化したファームウェア暗号化データを、CPU9内のブートROM21の暗号化処理部で共通鍵を用いて復号し、フラッシュROM22に書き込むことで、外部にファームウェアデータが漏洩することを防ぐことができる。

【0114】また、図4に示したフローチャートでは、暗号化されたファームウェア暗号化データをPC10から受信し、受信したファームウェア暗号化データを解読してフラッシュROM22に書き込む手法について記載しているが、PC10から暗号化されていないデータが送信された場合は、図5に示すように、図4のステップS25～ステップS27の工程をステップS25aのように、バッファメモリ8から直接フラッシュROM22に直接書き込むよう変更することで実行することが可能となる。

【0115】次に、図6に示すフローチャートを用いて、フラッシュROM22にファームウェアをアップデートした結果をPC10で検証する際の処理動作について説明をする。

【0116】ステップS41において、PC10は、フラッシュROM22に格納されているファームウェアの転送を要求するReadバッファコマンド(Read Buffer Command)をDVD-ROMドライブへ送信する。

【0117】ステップS42において、PC10から送信されたReadバッファコマンドを受信したことに応じて、CPUコア20は、フラッシュROM22の先頭アドレスからフラッシュROM22に記憶されているファームウェアの2KB分のデータを読み出す。

【0118】ステップS43において、CPUコア20は、読み出した2KB分のデータを、RAM23又は当該CPUコア20のレジスタに書き込み記憶させる。

【0119】ステップS44において、CPUコア20は、ブートROM21の暗号化処理部21aを制御し、共通鍵を用いて暗号化処理部21aに格納されている暗号解読アルゴリズムに従って、RAM23又は当該CP

Uコア20のレジスタに記憶されている2KB分のファームウェアデータを読み出して暗号化する。

【0120】ステップS45において、CPUコア20は、暗号化した2KB分のファームウェアデータをバッファメモリ8へ転送し、格納させる。

【0121】ステップS46において、CPUコア20は、フラッシュROM22に格納されているファームウェアデータを全て読み出したかどうかを検出する。ファームウェアデータを全て読み出した場合は工程をステップS47へと進め、まだ、全てのファームウェアデータが読み出されていない場合は工程をステップS42へと戻す。

【0122】ステップS47において、フラッシュROM22に格納されているファームウェアデータが全て読み出され、暗号化されてバッファメモリ8に格納されたことに応じて、CPUコア20は、バッファメモリ8に格納されているファームウェア暗号化データをPC10へと転送する。

【0123】転送されたファームウェア暗号化データは、PC10にて暗号化されたまま、元データと比較され一致が確認される。

【0124】このようにしてPC10は、DVD-ROMドライブのフラッシュROM22にファームウェアが確実に更新されているかどうかを検証することができる。その際に、CPU9内でファームウェアは暗号化されPC10へと送信されるので、途中の送信経路などで平文のファームウェアを入手することはできないため、ファームウェアの解析や改竄などを防ぐことができる。

【0125】また、上述したように、図1の構成のDVD-ROMドライブのCPU9ではファームウェア暗号化データの復号をブートROM21に記憶されている暗号解読アルゴリズムというプログラムで実行しているが、図7に示すようにプログラムである暗号処理部を共通鍵暗号化処理部32のようにハードウェア化して、CPU9を再構成してもよい。

【0126】このように共通鍵暗号化処理部32を備えるCPU9は、暗号化処理が高速となるため、ファームウェアのアップデートをより高速に実行させることができる。その際のアップデート処理の動作は、上述の図3、図4で示したフローチャートと同様の動作であるため省略をする。

【0127】上述の説明では、図1に示したようにPC10から送信される暗号化されたファームウェアを、CPU9自身で解読し、CPU9に備えられたフラッシュROM22にアップロードする構成となっていた。CPU9は、暗号化されたファームウェアを解読する暗号化処理部としてブートROM21を備えている。

【0128】このように、CPU9に備えられたブートROM21のように暗号化されたファームウェアの暗号を解読する暗号化処理部を図1で示したDVDデコーダ

7に搭載することも可能である。暗号化処理部を搭載するようにDVDデコーダ7をカスタマイズすることは、より現実的な構成であるといえる。

【0129】図8に第2の実施の形態として示す、DVDデコーダに暗号化されたファームウェアを解読する復号部17を搭載させたDVD-ROMドライブについて説明をする。

【0130】図8に示したDVD-ROMドライブにおけるDVDデコーダ7は、PC10から入力される暗号化されたファームウェアを解読するための復号部17と、フラッシュROM38に格納された平文のファームウェアをPC10にて検証する際に暗号化する暗号化部18とが、図1で示したDVDデコーダ7に付加された構成となっている。

【0131】復号部17、暗号化部18は、暗号化の手法として、キーストリーム（鍵ストリーム）と呼ばれる乱数（擬似乱数）を暗号化鍵として平文を暗号化する共通鍵暗号の1つであるストリーム暗号を解析することができる。ストリーム暗号方式による暗号化及び復号は、1ビット又は数ビット（例えば、1バイト）の小データブロックごとに逐次行われる。

【0132】復号部17は、ストリーム暗号に対応している場合は、図9に示すようにSEEDデータ格納部17aと、乱数生成部17bと、排他的論理和演算部17cとを備えている。

【0133】SEEDデータ格納部17aは、乱数生成部17bの初期入力値であり共通鍵に相当するSEEDデータを格納しており、CPUコア36からの指示に応じて格納しているSEEDデータを乱数生成部17bに出力する。

【0134】また、SEEDデータ格納部17aに格納されるSEEDデータは、固定された値があらかじめ格納されていてもよいし、CPUコア36から適時、設定可能としてもよい。

【0135】乱数生成部17bは、SEEDデータ格納部17aからSEEDデータが入力されたことに応じて所定のアルゴリズムで乱数を生成し、排他的論理和演算部17cに出力する。

【0136】排他的論理和演算部17cは、バッファメモリ8から所定のデータ長単位で読み出される、暗号化されたファームウェアデータであるファームウェア暗号化データと、上記乱数生成部17bから出力される乱数とで排他的論理和をとることで復号し、復号された平文のファームウェアデータをCPU35内のフラッシュROM38へと出力する。

【0137】暗号化部18は、ストリーム暗号に対応している場合は、図10に示すようにSEEDデータ格納部18aと、乱数生成部18bと、排他的論理和演算部18cとを備えている。

【0138】SEEDデータ格納部18aは、乱数生成

部18bの初期入力値であり共通鍵に相当するSEEDデータを格納しており、CPUコア36からの指示に応じて格納しているSEEDデータを乱数生成部18bに出力する。

【0139】また、SEEDデータ格納部18aに格納されるSEEDデータは、固定された値があらかじめ格納されていてもよいし、CPUコア36から適時、設定可能としてもよい。

【0140】なお、SEEDデータ格納部18aから乱数生成部18bに入力されるSEEDデータは、上述した復号部17において、SEEDデータ格納部17aから乱数生成部17bに入力されるSEEDデータと同じデータである。

【0141】乱数生成部18bは、SEEDデータ格納部18aからSEEDデータが入力されたことに応じて所定のアルゴリズムで乱数を生成し、排他的論理和演算部18cに出力する。

【0142】なお、乱数生成部18aで乱数生成に用いるアルゴリズムは、上述した復号部17の乱数生成部17bで乱数生成に用いるアルゴリズムと同じものである。

【0143】排他的論理和演算部18cは、フラッシュメモリ38から所定のデータ長単位で読み出される、平文のファームウェアデータと、上記乱数生成部18bから出力される乱数とで排他的論理和をとることで暗号化し、暗号化されたファームウェア暗号化データをバッファメモリ8へと出力する。

【0144】CPU35は、CPUコア36と、RAM37と、フラッシュROM38とを備えている。CPU35は、CPU I/F16を介してDVDデコーダ7'と接続されている。

【0145】CPUコア36は、図1で示したCPUコア20と同様に、CPU35の中心部分で四則演算や比較判断をする論理演算装置や加算回路、レジスタなどを備えている。

【0146】RAM37は、図1で示したRAM23と同様に、記憶内容維持のためのリフレッシュ動作が不要で高速アクセス可能なSRAMなどであり、フラッシュROM38内に格納されているファームウェアをアップデートする際にデータ及びアップデート用プログラムの展開領域となる。

【0147】フラッシュROM38は、例えば、データの電氣的消去が可能なプログラマブルROMであるEEPROMなどのいわゆるフラッシュメモリである。フラッシュROM38は、図1で示したフラッシュROM22と同様に、当該DVD-ROMドライブの再生制限をするプログラムであるファームウェアが格納される。

【0148】DVDデコーダ7'の復号部17で復号された平文のファームウェアデータは、CPU I/F16を介してCPU35内のフラッシュROM38に出力

される。

【0149】なお、フラッシュROM38でも、図1に示したDVD-ROMドライブのCPU9内に備えられたフラッシュROM22と同様にTMR素子を用いたMRAMを使用することも可能である。

【0150】図8に示したDVD-ROMドライブでは、DVDデコーダ7'で復号された平文のファームウェアデータは、平文のままCPU35に転送されることになる。そのため、転送される際に配線などが操作され、平文のファームウェアデータが盗み見られてしまう可能性がある。

【0151】したがって、平文のファームウェアが流れる箇所であるDVDデコーダ7'と、CPU35との間の配線を、多層基板を使って内層に施すようにしたり、半導体パッケージをピンのでないボールグリッドアレイなどにするとといった処理が必要となる。

【0152】なお、図8に示したDVD-ROMドライブのDVDデコーダ7'、CPU35以外の機能部に関しては、図1に示したDVD-ROMドライブが備える機能部と同じであるため説明を省略する。

【0153】次に、図11、図12に示すフローチャートを用いて、フラッシュROM38に記憶されたファームウェアをアップデートする際の動作について説明をする。まず、図11に示すフローチャートを用いて、アップデート(update)関数がRAM37に読み込まれるまでの動作について説明をする。

【0154】ステップS101において、CPUコア36は、PC10から送信され、受信したコマンドがWriteバッファコマンド(Write Buffer Command)であるかどうかを判定する。Writeバッファコマンドでない場合は工程をステップS102へ進め、Writeバッファコマンドである場合は工程をステップS103へと進める。

【0155】ステップS102において、CPUコア36は、PC10から送信されたWriteバッファコマンドに、フラッシュROM38に記憶されているファームウェアを更新することを指示するパラメータが付加されているかどうかを検出し、付加されていない場合は工程をステップS103へと進め、付加されている場合は工程をステップS104へと進める。

【0156】ステップS103において、CPUコア36は、PC10から送信されたコマンドがWriteバッファコマンドでなかったことに応じて、送信されたコマンドを実行する。また、CPUコア36は、送信されたコマンドが、Writeバッファコマンドであったがファームウェアを更新することを指示するパラメータが付加されていないことに応じて、PC10から送信されるファームウェア以外のデータをバッファメモリ8に書き込むよう制御をする。ステップS103の工程が終了すると工程は、ステップS101へと戻る。

【0157】PC10は、DVD-ROMドライブにWriteバッファコマンドを送信した後、更新するファームウェアをストリーム暗号化方式で暗号化したファームウェア暗号化データをバイナリーファイルとしてDVD-ROMドライブに送信する。

【0158】ステップS104において、CPUコア36は、Writeバッファコマンドを受信したことに応じて、バッファメモリ8のデータ記憶領域の所定のアドレスNからM（Mは自然数）Byte分の領域を確保し、PC10から送信されるバイナリーファイルを上記確保したデータ記憶領域に記憶させる。

【0159】ステップS105において、CPUコア36は、転送されたバイナリーファイルのChecksumを確認する。送信されるバイナリーファイルには、Checksumデータが添付されている。CPUコア36は、この添付されたChecksumデータと、送信されたバイナリーファイルのバイナリーデータの加算値とを比較し、一致した場合は正しくバイナリーファイルが送信されたとして工程をステップS107へと進め、一致しなかった場合はバイナリーファイルの送信が失敗したとして工程をステップS106に進める。

【0160】ステップS106において、CPUコア36は、ステップS105でのChecksumデータの検証結果から正しくバイナリーファイルが送信されなかったことを、Check Condition Statusにてコマンドを完了させることでPC10に知らせ、工程を再びステップS101へと戻す。

【0161】ステップS107において、CPUコア36は、フラッシュROM38に格納されているフラッシュROM38のファームウェアを更新するアップデート関数をRAM37にコピーし、RAM37でCPUコア36のプログラムを実行できる状態にする。

【0162】その後、CPUコア36は、フラッシュROM38のファームウェア格納領域に記憶されているデータ、つまり更新前のファームウェアを消去する。なお、この消去動作は、フラッシュROM38がオーバーライト可能なMRAMであった場合、省略されることになる。

【0163】続いて、図12に示すフローチャートを用いてアップデート（update）関数による処理動作について説明をする。

【0164】ステップS111において、CPUコア36は、RAM37に格納されたアップデート関数の先頭アドレスにアクセスし、アップデート関数によるファームウェアのフラッシュROM38へのアップデートを開始する。

【0165】ステップS112において、CPUコア36は、図示しない割り込み制御回路を制御して全ての割り込みプログラムの実行と、例外処理の実行を禁止す

る。

【0166】ステップS113において、CPUコア36は、フラッシュROM38への書き込みタイミングを制御する図示しない書き込みタイミング制御用タイマーを起動する。以下、フラッシュROM38へデータを書き込む際は、書き込みタイミング制御用タイマーのタイミング制御に基づいて実行される。

【0167】ステップS114において、CPUコア36は、ファームウェア暗号化データのバイナリファイルが記憶されているバッファメモリ8のアドレス番号Nと、ファームウェアを記憶させるフラッシュROM38のアドレス番号0にアクセスをする。

【0168】ステップS115において、CPUコア36は、バッファメモリ8のアドレス番号Nから復号に都合のよい単位ごと（例えば、1Byteのデータ）に読み出し、復号部17で復号処理をして平文にする。CPUコア36は、復号され平文であるファームウェアデータを、当該CPUコア36内のレジスタ又はRAM37に格納する。

【0169】さらに、CPUコア36は、当該CPUコア36内のレジスタ又はRAM37に格納されたファームウェアデータを読み出し、フラッシュROM38のアドレス番号0から書き込む。

【0170】ステップS116において、CPUコア36は、フラッシュROM38にファームウェアデータが全て書き込まれたかどうかを判断する。CPUコア36は、アドレス番号がMでない場合には工程をステップS117へと進め、アドレス番号がMとなったら工程をステップS118に進める。

【0171】ステップS117において、CPUコア36は、バッファメモリ8のアドレス番号及びフラッシュROM38のアドレス番号を1Byte増やしたアドレス番号へアクセスをする。この工程が終了するとステップS115へと戻り、バッファメモリ8のアクセスしたアドレス番号からファームウェア暗号データを読み出し、復号処理をして復号された平文のファームウェアデータをフラッシュROM38のアクセスしたアドレス番号に書き込む。

【0172】ステップS118において、CPUコア36は、フラッシュROM38への書き込みタイミングを制御する図示しない書き込みタイミング制御用タイマーを停止させる。

【0173】ステップS119において、ステップS116で、フラッシュROM38に記憶されたファームウェアデータの最終アドレス番号がMであると判定され、ステップS118で、図示しない書き込みタイミング制御用タイマーが停止されたことで、ファームウェアのフラッシュROM38へのアップデートが完了する。

【0174】このようにして、本発明を適用した図8に示すDVD-ROMドライブでは、フラッシュROM3

8に格納されているファームウェアをアップデートする際、PC10でストリーム暗号方式で暗号化されたファームウェア暗号化データを、DVDデコーダ7'内の復号部17で復号し、CPU35内のフラッシュROM38に書き込む。

【0175】DVDデコーダ7'と、CPU35とのやり取りでは、平文のファームウェアデータが転送されることになるが、配線処理や半導体パッケージの端子部分が露出しないといった実装レベルの工夫をすることで、ファームウェアデータの漏洩を防ぐことができる。

【0176】次に、図13に示すフローチャートを用いて、フラッシュROM38にファームウェアをアップデートした結果をPC10で検証する際の処理動作について説明をする。

【0177】ステップS121において、CPUコア36は、PC10から送信され、受信したコマンドがReadバッファコマンド(Read Buffer Command)であるかどうかを判定する。Readバッファコマンドでない場合は工程をステップS123へ進め、Readバッファコマンドである場合は工程をステップS122へと進める。

【0178】ステップS122において、CPUコア36は、PC10から送信されたReadバッファコマンドに、フラッシュROM38に記憶されているファームウェアを読み出すことを指示するパラメータが付加されているかどうかを検出し、付加されていない場合は工程をステップS123へと進め、付加されている場合は工程をステップS124へと進める。

【0179】ステップS123において、CPUコア36は、PC10から送信されたコマンドがReadバッファコマンドでなかったことに応じて、送信されたコマンドを実行する。また、CPUコア36は、送信されたコマンドが、Readバッファコマンドであったがファームウェアを更新することを指示するパラメータが付加されていなかったことに応じて、ファームウェア以外のデータをバッファメモリ8に読み出すよう制御をする。ステップS123が終了すると工程は終了する。

【0180】PC10は、DVD-ROMドライブにReadバッファコマンドを送信した後、更新するファームウェアをストリーム暗号化方式で暗号化したファームウェア暗号化データをバイナリーファイルとしてDVD-ROMドライブに送信する。

【0181】ステップS124において、CPUコア36は、バッファメモリ8のアドレス番号Nと、ファームウェアが記憶されているフラッシュROM38のアドレス番号0にアクセスをする。

【0182】ステップS125において、CPUコア36は、フラッシュROM38のアドレス番号0から復号に都合のよい単位ごと(例えば、1Byteのデータ)に読み出し、当該CPUコア36内のレジスタ又はRAM37に格納する。

M37に格納する。

【0183】さらに、CPUコア36は、当該CPUコア36内のレジスタ又はRAM37に格納された平文であるファームウェアデータを読み出し、DVDデコーダ7'の暗号化部18で暗号化処理をしてファームウェア暗号化データにする。CPUコア36は、暗号化されたファームウェア暗号化データをバッファメモリ8のアドレス番号Nから書き込む。

【0184】ステップS126において、CPUコア36は、フラッシュROM38からファームウェアデータが全て読み出されたかどうかを判断する。CPUコア36は、アドレス番号がMでない場合には工程をステップS127へと進め、アドレス番号がMとなった工程をステップS128に進める。

【0185】ステップS127において、CPUコア36は、バッファメモリ8のアドレス番号及びフラッシュROM38のアドレス番号を1Byte増やしたアドレス番号へアクセスをする。この工程が終了するとステップS125へと戻り、フラッシュROM38のアクセスしたアドレス番号からファームウェアデータを読み出し、暗号化処理をして暗号化されたファームウェア暗号化データをバッファメモリ8のアクセスしたアドレス番号に書き込む。

【0186】ステップS128において、フラッシュROM38に格納されているファームウェアデータが全て読み出され、暗号化されてバッファメモリ8に格納されたことに応じて、CPUコア36は、バッファメモリ8に格納されているファームウェア暗号化データをPC10へと転送する。

【0187】転送されたファームウェア暗号化データは、PC10にて暗号化されたまま元データと比較され一致が確認される。

【0188】このようにして、PC10は、DVD-ROMドライブのフラッシュROM38にファームウェアが確実に更新されているかどうかを検証することができる。

【0189】DVDデコーダ7'と、CPU35とのやり取りでは、平文のファームウェアデータが転送されることになるが、配線処理や半導体パッケージの端子部分が露出しないといった実装レベルの工夫をすることで、ファームウェアデータの漏洩を防ぐことができる。

【0190】ところで、一般に、PC(Personal Computer)などにおいて実行されるプログラムは、HD(Hard Disk)などの補助記憶装置に記憶されており、PCの電源起動時にRAM(Random Access Memory)などの主記憶装置にロードされる。CPUは、主記憶装置にロードされたプログラムを読み込んで、プログラムの実行をする。

【0191】このように、CPUが実行するプログラムを主記憶装置にロードするには、CPUコア内に常駐、

又は、上記HDから最初に読み込まれるIPL (Initial Program Loader) によって行われる。

【0192】一方、第1の実施の形態として図1を用いて説明したDVD-ROMドライブ、及び第2の実施の形態として図8を用いて説明したDVD-ROMドライブでは、DVDデコーダにCPUを備えている場合がある。このように、DVDデコーダに備えられたCPUも上述したPCと同様に外部の記憶部に格納されているプログラムをRAMに読み出し、RAMに読み出したプログラムを実行させることでDVDデコードなどの所定の処理を行うことになる。

【0193】したがって、外部の記憶部に格納されているプログラムは、DVDデコーダ内のRAMに読み出される際、盗み見られ、プログラムの解析や改竄といった行為がなされてしまう可能性があるため暗号化して格納されている必要がある。

【0194】なお、以下の説明においては、DVDデコーダが備えるCPUが実行するプログラムをマイクロプログラムと呼び、そのデータをマイクロプログラムデータと呼ぶ。また、マイクロプログラムデータが暗号化されたものは暗号化マイクロプログラムデータと呼ぶ。

【0195】図14に第3の実施の形態として示すDVD-ROMドライブでは、DVDデコーダとして、図1で示したDVDデコーダ7に、内部CPUコア41と、SRAM42と、復号部43とを付加したDVDデコーダ7"を備えている。内部CPUコア41、SRAM42、復号部43は、メモリ制御部14、CPU I/F16と内部バスで接続されている。また、図14に示したDVD-ROMドライブでは、外部CPU45と、DVDデコーダ7"に読み込まれる暗号化されたマイクロプログラムデータ (暗号化マイクロプログラムデータ) が格納されたフラッシュROM46とを備えている。

【0196】内部CPUコア41は、DVDデコーダ7"制御用のマイクロコントローラである。内部CPUコア41は、自身が実行するマイクロプログラムをSRAM42に読み込ませるためのプログラムであるIPLを格納している。DVD-ROMドライブに電源が投入されるとIPLが起動することになる。

【0197】SRAM42は、内部CPUコア41で実行するマイクロプログラムデータを格納する内部CPUコア41に対する主記憶装置である。SRAM42には、IPLによってフラッシュROM46から読み出された暗号化マイクロプログラムデータが復号部43で復号されて格納される。

【0198】復号部43は、フラッシュROM46に格納されている暗号化されたマイクロプログラムデータ (暗号化マイクロプログラムデータ) を復号してSRAM42のプログラム領域へ転送するための復号回路である。復号部43は、共通鍵暗号 (ブロック暗号、ストリーム暗号) 化方式で暗号化されたマイクロプログラムデータ

(暗号化マイクロプログラムデータ) を復号する。

【0199】復号部43は、ストリーム暗号に対応している場合は、図15に示すようにSEEDデータ格納部43aと、乱数生成部43bと、排他的論理和演算部43cとを備えている。

【0200】SEEDデータ格納部43aは、乱数生成部43bの初期入力値であり共通鍵に相当するSEEDデータを格納しており、内部CPUコア41からの指示に応じて格納しているSEEDデータを乱数生成部43bに出力する。

【0201】また、SEEDデータ格納部43aに格納されるSEEDデータは、固定された値があらかじめ格納されていてもよいし、内部CPUコア41から適時、設定可能としてもよい。

【0202】乱数生成部43bは、SEEDデータ格納部43aからSEEDデータが入力されたことに応じて所定のアルゴリズムで乱数を生成し、排他的論理和演算部43cに出力する。

【0203】排他的論理和演算部43cは、フラッシュROM46から所定のデータ長単位で読み出される、暗号化されたマイクロプログラムデータである暗号化マイクロプログラムデータと、上記乱数生成部43bから出力される乱数とで排他的論理和をとることで復号し、復号された平文のマイクロプログラムデータをDVDデコーダ7"内のSRAM42へと出力する。

【0204】また、DVDデコーダ7"のCPU I/F16は、当該DVDデコーダ7"内のSRAM42に格納されているマイクロプログラムデータ、復号部43のSEEDデータ格納部43aに格納されているSEEDデータ、乱数生成部43bの乱数生成アルゴリズムをユーザレベルでは参照できないような保護機能を備えている。これにより、復号された平文のマイクロプログラムデータ、及び、暗号化マイクロプログラムデータを復号するための復号機能を取り出すことを制限することができる。

【0205】外部CPU45は、DVD-ROMドライブを統括的に制御する制御部であり、四則演算や比較判断をする論理演算装置や加算回路、レジスタなどを備えている。

【0206】フラッシュROM46は、例えば、データの電氣的消去が可能なプログラマブルROMであるEEPROMなどのいわゆるフラッシュメモリである。フラッシュROM46は、内部CPUコア41の実行プログラムが暗号化された暗号化マイクロプログラムデータを格納している。

【0207】続いて、図16に示すフローチャートを用いて、図14に示すDVD-ROMドライブの起動時の動作について説明をする。

【0208】ステップS131において、電源投入リセットにより、内部CPUコア41内に常駐するIPLが

起動する。IPLが起動すると同時に、復号部43では、SEEDデータを乱数生成部43bが取り込むことで初期化が行われる。

【0209】ステップS132において、内部CPUコア41で実行されるIPLによって、フラッシュROM46の先頭アドレスから、当該フラッシュROM46に格納されている暗号化マイクロプログラムデータの読み出しが開始される。読み出された暗号化マイクロプログラムデータは、復号部43に入力され乱数生成部43aからの出力データと排他的論理和をとって平文であるマイクロプログラムデータに復号される。復号されたマイクロプログラムデータは、SRAM42に書き込まれる。

【0210】ステップS133において、内部CPUコア41で実行されるIPLによって、フラッシュROM46内に格納されている暗号化マイクロプログラムデータが所定の量だけ読み出されたかどうか判定される。所定量の暗号化マイクロプログラムデータが読み出された場合は、工程をステップS134へと進め、所定量の暗号化マイクロプログラムデータが読み出されていない場合は、フラッシュROM46からの読み出し、復号部43での復号、SRAM42への書き込みが実行される。

【0211】ステップS134において、内部CPUコア41で実行されるIPLによって、フラッシュROM46からの読み出しが完了すると、内部CPUコア41は、内蔵するプログラムカウンタの値をSRAM42の先頭アドレスとし、SRAM42内に書き込まれた平文であるマイクロプログラムデータを実行する。

【0212】このようにして、フラッシュROM46に格納されている暗号化マイクロプログラムデータは、図14に示すDVD-ROMドライブが起動するとともにIPLによって読み出され、DVDデコーダ7'内で復号され、SRAM42に書き込まれる。したがって、DVDデコーダ7'内部CPUコア41が実行するマイクロプログラムは、当該DVDデコーダ7'内で暗号が復号されるため、プログラムの解析や改竄を防止することができる。

【0213】上述したように、DVD-ROMドライブのファームウェアを更新する際、暗号化してPC10からDVD-ROMドライブへ転送し、図1に示したCPU9内、又は、図8に示したDVDデコーダ7'内で復号してCPU内のフラッシュROMに更新することで、更新時の解析や改竄を防止することができる。また、図14に示したDVD-ROMドライブのように起動時にロードするプログラムも暗号化したまま復号する回路内に読み出し、当該回路内で暗号を復号することでロード時のプログラムの解析や改竄を防止することができる。

【0214】なお、図14を用いて説明したDVD-ROMドライブにおいて、SRAM42へ格納するマイクロプログラムは、DVDデコーダ7'にバスで接続され

たフラッシュROM46から供給されるとしているが、例えば、読み出し専用ROM、ディスク状記録媒体、リムーバブル半導体メモリなど、どんなものであってもかまわない。

【0215】また、図14を用いて説明したDVD-ROMドライブでは、フラッシュROM46から復号部43を経由したSRAM42へのマイクロプログラムの読み出し処理を、DVDデコーダ7'に内蔵されている内部CPUコア41が備えるIPLによって実行していたが、DVDデコーダ7'の外部にあるCPU、例えば、外部CPU45などの制御によって実施するようにしてもよい。

【0216】しかし、上述したように暗号化されたプログラムの復号後のデータ漏洩を防止できたとしても、暗号化されたままプログラムが改竄されるということも考えられる。

【0217】例えば、図1に示したDVD-ROMドライブで、ファームウェアが暗号化されたまま改竄されると、フラッシュROM22には、そのまま改竄されたデータが格納されてしまうことになり、コンテンツの違法複製、ドライブの動作不良などを引き起こしてしまう可能性がある。

【0218】そこで、更新するプログラム本体にプログラムが改竄されたことを検証する検証プログラムを添付してDVD-ROMドライブに送信するといった手法が考えられる。更新するプログラム本体にこの検証プログラムを添付すると、DVD-ROMドライブで更新されたプログラムを実行すると、まずプログラム本体に添付した検証プログラムが起動し、更新されたプログラムが改竄されているか否かを検証することができる。

【0219】図17、図18、図19に示すフローチャートを用いて、上述した暗号化データの改竄を防止して、プログラムの更新をする動作について説明をする。なお、説明のためプログラムを更新するドライブとして図8に示したDVD-ROMドライブを用いる。

【0220】まず、図17に示したフローチャートを用いて検証プログラムを添付したプログラム本体をDVD-ROMドライブに送信するまでの動作について説明をする。

【0221】ステップS141において、例えば、ドライブ製造会社などによってDVD-ROMドライブに送信するプログラムが作成される。作成されるプログラム本体には、上述したプログラムの改竄を検証するための検証プログラムが添付されている。

【0222】ステップS142において、ドライブ製造会社は、配布するプログラムから検証データを生成し、図20に示すように生成した検証データをプログラムに付加する。

【0223】この検証データは、ハッシュ関数を用いてプログラム本体を演算することで得られるハッシュ値で

ある。例えば、図21に示すようにハッシュ関数として、米国商務省に所属する標準化機関NISTによって定められたハッシュアルゴリズムであるSHA (Secure Hash Algorithm) をさらに改良したSHA-1を使用することができる。SHA-1は、 2^{64} ビット未満のデータ長から160ビット長のハッシュ値(検証データ)を生成するアルゴリズムである。

【0224】ステップS143において、ドライブ製造会社は、検証データが付加されたプログラムを、図22に示すように検証データも含めて暗号化する。

【0225】ステップS144において、ドライブ製造会社は、暗号化されたプログラムからCheck Sumデータを算出し、図23に示すようにCheck Sumデータを付加する。付加するデータは、Check Sumデータに代えて、再びハッシュ関数により求めたハッシュ値であってもよい。Check Sumデータが付加されることでプログラムは、送信可能なデータとなる。

【0226】送信可能なデータは、例えば、ROMメディアなどを使って、ユーザ(PC10)に配布される。

【0227】ステップS145において、PC10は、DVD-ROMドライブに送信可能となったデータ(プログラム)を送信する。

【0228】次に、図18に示すフローチャートを用いて、PC10から送信された暗号化データの改竄防止措置がなされたプログラムを受信するDVD-ROMドライブの動作について説明をする。

【0229】ステップS151において、DVD-ROMドライブは、PC10からWriteバッファコマンドとともに送信されるプログラムを受信すると、プログラムに添付されたCheck Sumデータと、送信されたプログラム暗号化データの加算値とを比較する。一致しなかった場合は工程をステップS152へと進め、一致した場合は工程をステップS153へと進める。

【0230】ステップS152において、Check Sumデータの比較結果から正しくプログラム暗号化データが送信されなかったことをCheck Condition Statusにてコマンド完了することでPC10に知らせ、工程を再びステップS151へと戻す。

【0231】ステップS153において、復号部17は、プログラム暗号化データを復号する。復号されたデータには検証データが付加されており、プログラム本体には検証プログラムが記述されている。

【0232】ステップS154において、復号されたプログラムデータは、フラッシュROM38に格納される。

【0233】ステップS155において、フラッシュROM38に格納されたプログラムが起動すると、まず始めに検証プログラムが動作する。

【0234】次に、図19に示すフローチャートを用いて、検証プログラムの動作を説明する。

【0235】ステップS161において、起動した検証プログラムは、プログラム本体のハッシュ値をハッシュ関数により計算する。

【0236】ステップS162において、検証プログラムは、ハッシュ値が計算されるとプログラム本体に添附された検証データと、計算されたハッシュ値と比較し、一致した場合は工程をステップS163へと進め、一致しなかった場合は工程をステップS164へと進める。

【0237】ステップS163において、DVD-ROMドライブは、添附された検証データと、計算したハッシュ値とが一致し、フラッシュROM38に格納されたプログラムが改竄されていないプログラムであると判定されたことに応じて、フラッシュROM38に格納されたプログラム本体を実行する。

【0238】ステップS164において、DVD-ROMドライブは、添附された検証データと、計算したハッシュ値とが一致せず、フラッシュROM38に格納されたファームウェアが改竄されたプログラムであると判定されたことに応じて、Not Ready状態となり、何も動作しない安定な状態となる。

【0239】このようにして、送信するプログラム本体に、ハッシュ関数によって算出された検証データを付加して送信することで、DVD-ROMドライブは、暗号化データそのものが改竄された場合であっても改竄されたことを検証することができる。

【0240】なお、上述した本発明の第1の実施の形態、第2の実施の形態として示すDVD-ROMドライブでは、ファームウェアを更新する際、更新するファームウェアをPC10から送信されるようにしているが、ファームウェアは、例えば、当該DVD-ROMドライブで再生可能なDVD-ROM1に記録されていてもよい。DVD-ROM1にファームウェア暗号化データをファイルとして記憶することで、DVD-ROMドライブは、このDVD-ROM1を再生することによって更新するファームウェアを取得することができる。

【0241】同様に、本発明の第3の実施の形態として示すDVD-ROMドライブでは、暗号化マイクロプログラムデータをファイルとして記録したDVD-ROM1を再生することによってマイクロプログラムをロードするようにしてもよい。

【0242】また、このDVD-ROM1には、本発明の第1の実施の形態として示したDVD-ROMドライブのブートROM21に書き込まれているファームウェア更新時に起動するプログラムが書き込まれていてもよく、上述のようにDVD-ROMドライブはDVD-ROM1を再生することでファームウェアを更新させることができる。

【0243】同様に、DVD-ROM1には、本発明の

第2の実施の形態として示したDVD-ROMドライブでファームウェア更新時に起動するプログラムが書き込まれてもよく、上述のようにDVD-ROMドライブはDVD-ROM1を再生することでファームウェアを更新させることができる。

【0244】同様に、DVD-ROM1には、本発明の第3の実施の形態として示したDVD-ROMドライブでマイクロプログラムをロードする時に起動するプログラムが書き込まれてもよく、上述のようにDVD-ROMドライブはDVD-ROM1を再生することでマイクロプログラムをロードさせることができる。

【0245】また、本発明の第1の実施の形態及び第2の実施の形態として示したDVD-ROMドライブにおいて、メモリスティック（登録商標）などのリムーバブル半導体メモリーに対応した半導体メモリー用スロットを設け、上述したDVD-ROM1の代わりにファームウェア暗号化データを上記リムーバブル半導体メモリーへ記録してファームウェアを更新するようにしてもよい。

【0246】同様に、本発明の第3の実施の形態として示したDVD-ROMドライブでも、暗号化マイクロプログラムデータを上記リムーバブル半導体メモリーへ記録してマイクロプログラムをロードするようにしてもよい。

【0247】さらにまた、上述のように本発明の第1の実施の形態、第2の実施の形態及び第3の実施の形態としてDVD-ROMドライブを適用しているが、本発明はこれに限定されるものではなく、CD-ROM、データが記録されたCD-R、CD-RW、DVD-RAM、DVD-R/RW、DVD+R/RWを記録再生可能なディスク装置全般に適用することが可能である。

【0248】また、本発明を適用した第1の実施の形態、第2の実施の形態及び第3の実施の形態としてDVD-ROMドライブを用いたが、本発明はこれに限定されるものではなく、何らかのセキュリティが必要な処理装置全般に適用可能である。

【0249】また、ファームウェア又はマイクロプログラムを暗号化し、復号する手法として共通鍵を用いた暗号化手法を用いているが、本発明はこれに限定されるものではなく、公開鍵方式やそれ以外の暗号化アルゴリズムを適用してもかまわない。

【0250】さらにまた、本発明を適用した第1の実施の形態、第2の実施の形態及び第3の実施の形態として示したDVD-ROMドライブでは、ファームウェアや、マイクロプログラムを対象としていたが、当該DVD-ROMドライブ内の書き換え可能なレジスタ・メモリの設定値というようにデータを対象とし、更新又は設定などをしてもよい。

【0251】

【発明の効果】以上の説明からも明らかなように、本発明の情報処理装置は、復号手段で、暗号化プログラムデータを所定の復号鍵を用いてプログラムに復号し、復号

したプログラムを記憶手段に記憶させ、記憶したプログラムを読み出し、読み出したプログラムに基づいて制御手段で当該情報処理装置の所定の動作を制御することで、プログラムロード時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムをロードする際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【0252】例えば、DVD-ROMドライブのファームウェアを更新することでファームウェアデータが漏洩した場合に生ずるリージョナルコード（RC：Regional Code）による再生制限の無効化や、DVD-ROMの違法コピー及び違法コピーDVD-ROMの再生制限の無効化といった違法行為を防止することが可能となる。

【0253】また、以上の説明からも明らかなように、本発明のプログラムロード方法は、復号ステップで、暗号化プログラムデータを所定の復号鍵を用いてプログラムに復号し、復号したプログラムを記憶手段に記憶させ、記憶したプログラムを読み出し、読み出したプログラムに基づいて制御ステップで当該情報処理装置の所定の動作を制御することで、プログラムロード時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムをロードする際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【0254】例えば、DVD-ROMドライブのファームウェアを更新することでファームウェアデータが漏洩した場合に生ずるリージョナルコード（RC：Regional Code）による再生制限の無効化や、DVD-ROMの違法コピー及び違法コピーDVD-ROMの再生制限の無効化といった違法行為を防止することが可能となる。

【0255】また、以上の説明からも明らかなように、本発明の記録媒体は、復号ステップで、暗号化プログラムデータを所定の復号鍵を用いてプログラムに復号し、復号したプログラムを記憶手段に記憶させ、記憶したプログラムを読み出し、読み出したプログラムに基づいて制御ステップで当該情報処理装置の所定の動作を制御することを特徴とするプログラムを記録することで、プログラムロード時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムをロードする際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【0256】例えば、DVD-ROMドライブのファームウェアを更新することでファームウェアデータが漏洩した場合に生ずるリージョナルコード（RC：Regional Code）による再生制限の無効化や、DVD-ROMの違法コピー及び違法コピーDVD-ROMの再生制限の無効化といった違法行為を防止することが可能となる。

【0257】以上の説明からも明らかなように、本発明の情報処理装置は、プログラム更新要求に応じて、制御部内の復号手段で、第2のプログラムを所定の暗号化鍵

で暗号化した暗号化プログラムデータを所定の復号鍵を用いて第2のプログラムに復号し、プログラム書き込み手段で復号した第2のプログラムを記憶手段に書き込んで第1のプログラムを更新し、さらに、取り出し制限手段で復号手段で復号された第2のプログラム及び記憶手段に書き込まれた第2のプログラムの外部装置からの取り出しを制限することで、プログラム更新時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムを更新する際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【0258】例えば、DVD-ROMドライブのファームウェアを更新することでファームウェアデータが漏洩した場合に生ずるリージョナルコード(RC:Regional Code)による再生制限の無効化や、DVD-ROMの違法コピー及び違法コピーDVD-ROMの再生制限の無効化といった違法行為を防止することが可能となる。

【0259】また、本発明の情報処理装置は、制御部のアーキテクチャを新たに構築する必要がないため、安価に製造することができる。

【0260】さらに、本発明の情報処理装置は、プログラムの更新時にだけ制御部内で暗号復号処理をするので、通常時における制御部の処理動作を低下させることがない。

【0261】また、以上の説明からも明らかなように、本発明のプログラム更新方法は、プログラム更新要求に応じて、復号ステップで、第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを所定の復号鍵を用いて第2のプログラムに復号し、プログラム書き込みステップで復号した第2のプログラムを記憶手段に書き込んで第1のプログラムを更新し、さらに、取り出し制限ステップで復号ステップで復号された第2のプログラム及び記憶手段に書き込まれた第2のプログラムの外部装置からの取り出しを制限することで、プログラム更新時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムを更新する際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【0262】例えば、DVD-ROMドライブのファームウェアを更新することでファームウェアデータが漏洩した場合に生ずるリージョナルコード(RC:Regional Code)による再生制限の無効化や、DVD-ROMの違法コピー及び違法コピーDVD-ROMの再生制限の無効化といった違法行為を防止することが可能となる。

【0263】さらに、本発明のプログラム更新方法は、第1のプログラムの更新時にだけ制御部内で暗号復号処理をするので、通常時における制御部の処理動作を低下させることがない。

【0264】また、以上の説明からも明らかなように、本発明の記録媒体は、プログラム更新要求に応じて、復号ステップで、第2のプログラムを所定の暗号化鍵で暗

号化した暗号化プログラムデータを所定の復号鍵を用いて第2のプログラムに復号し、プログラム書き込みステップで復号した第2のプログラムを記憶手段に書き込んで第1のプログラムを更新し、さらに、取り出し制限ステップで復号ステップで復号された第2のプログラム及び記憶手段に書き込まれた第2のプログラムの外部装置からの取り出しを制限することでことを特徴とするプログラムを記録することで、プログラム更新時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムを更新する際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【0265】例えば、DVD-ROMドライブのファームウェアを更新することでファームウェアデータが漏洩した場合に生ずるリージョナルコード(RC:Regional Code)による再生制限の無効化や、DVD-ROMの違法コピー及び違法コピーDVD-ROMの再生制限の無効化といった違法行為を防止することが可能となる。

【0266】さらに、本発明の記録媒体に記録されたプログラムは、第1のプログラムの更新時にだけ制御部内で暗号復号処理をするので、通常時における制御部の処理動作を低下させることがない。

【0267】また、以上の説明からも明らかなように、本発明の回路素子は、プログラム更新要求に応じて、集積化された復号手段で第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを所定の復号鍵を用いて第2のプログラムに復号し、プログラム書き込み手段で復号した第2のプログラムを記憶手段に書き込んで第1のプログラムを更新し、さらに、取り出し制限手段で復号手段で復号された第2のプログラム及び記憶手段に書き込まれた第2のプログラムの外部装置からの取り出しを制限することで、プログラム更新時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムを更新する際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【0268】例えば、DVD-ROMドライブのファームウェアを更新することでファームウェアデータが漏洩した場合に生ずるリージョナルコード(RC:Regional Code)による再生制限の無効化や、DVD-ROMの違法コピー及び違法コピーDVD-ROMの再生制限の無効化といった違法行為を防止することが可能となる。

【0269】さらに、本発明の回路素子は、第1のプログラムの更新時にだけ当該回路素子内で暗号復号処理をするので、通常時における当該回路素子の処理動作を低下させることがない。

【0270】以上の説明からも明らかなように、本発明の情報処理装置は、プログラム更新要求に応じて、データ処理部内の復号手段で、第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを所定の復号鍵を用いて第2のプログラムに復号して制御部に送信し、制御部のプログラム書き込み手段で復号した第2の

プログラムを制御部内の記憶手段に書き込んで第1のプログラムを更新することで、プログラム更新時における外部へのプログラムデータの漏洩を少なくできるため、プログラムを更新する際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【0271】例えば、DVD-ROMドライブのファームウェアを更新することでファームウェアデータが漏洩した場合に生ずるリージョンコード(RC:Regional Code)による再生制限の無効化や、DVD-ROMの違法コピー及び違法コピーDVD-ROMの再生制限の無効化といった違法行為を防止することが可能となる。

【0272】また、以上の説明からも明らかなように、本発明のプログラム更新方法は、プログラム更新要求に応じて、復号ステップで、第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを所定の復号鍵を用いて第2のプログラムに復号して制御部に送信し、プログラム書き込みステップで復号した第2のプログラムを制御部内の記憶手段に書き込んで第1のプログラムを更新することで、プログラム更新時における外部へのプログラムデータの漏洩を少なくできるため、プログラムを更新する際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【0273】例えば、DVD-ROMドライブのファームウェアを更新することでファームウェアデータが漏洩した場合に生ずるリージョンコード(RC:Regional Code)による再生制限の無効化や、DVD-ROMの違法コピー及び違法コピーDVD-ROMの再生制限の無効化といった違法行為を防止することが可能となる。

【0274】また、以上の説明からも明らかなように、本発明の記録媒体は、プログラム更新要求に応じて、復号ステップで、第2のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを所定の復号鍵を用いて第2のプログラムに復号して制御部に送信し、プログラム書き込みステップで復号した第2のプログラムを制御部内の記憶手段に書き込んで第1のプログラムを更新することを特徴とするプログラムを記録することで、プログラム更新時における外部へのプログラムデータの漏洩を少なくできるため、プログラムを更新する際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【0275】例えば、DVD-ROMドライブのファームウェアを更新することでファームウェアデータが漏洩した場合に生ずるリージョンコード(RC:Regional Code)による再生制限の無効化や、DVD-ROMの違法コピー及び違法コピーDVD-ROMの再生制限の無効化といった違法行為を防止することが可能となる。

【0276】以上の説明からも明らかなように、本発明の情報処理装置は、データ処理部内の復号手段で、所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを所定の復号鍵を用いて所定のプログラム

に復号し、復号した所定のプログラムをデータ処理部内の記憶手段に記憶させ、取り出し制限手段で復号手段で復号された所定のプログラム及び記憶手段に記憶された所定のプログラムの外部装置からの取り出しを制限することで、プログラムロード時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムをロードする際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【0277】また、以上の説明からも明らかなように、本発明のプログラムロード方法は、復号ステップで、所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを所定の復号鍵を用いて所定のプログラムに復号し、復号した所定のプログラムをデータ処理部内の記憶手段に記憶させ、取り出し制限ステップで復号ステップで復号された所定のプログラム及び記憶手段に記憶された所定のプログラムの外部装置からの取り出しを制限することで、プログラムロード時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムをロードする際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【0278】また、以上の説明からも明らかなように、本発明の記録媒体は、復号ステップで、所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを所定の復号鍵を用いて所定のプログラムに復号し、復号した所定のプログラムをデータ処理部内の記憶手段に記憶させ、取り出し制限ステップで復号ステップで復号された所定のプログラム及び記憶手段に記憶された所定のプログラムの外部装置からの取り出しを制限することを特徴とするプログラムを記録することで、プログラムロード時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムをロードする際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【0279】また、以上の説明からも明らかなように、本発明の回路素子は、復号手段で、所定のプログラムを所定の暗号化鍵で暗号化した暗号化プログラムデータを所定の復号鍵を用いて所定のプログラムに復号し、復号した所定のプログラムを記憶手段に記憶させ、取り出し制限手段で復号手段で復号された所定のプログラム及び記憶手段に記憶された所定のプログラムの外部装置からの取り出しを制限することで、プログラムロード時における外部へのプログラムデータの漏洩を阻止することができるため、プログラムをロードする際に漏洩したプログラムデータを用いた違法行為を防止することが可能となる。

【図面の簡単な説明】

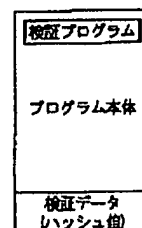
【図1】本発明の第1の実施の形態として示すDVD-ROMドライブの構成を説明するためのブロック図である。

【図2】暗号化について説明するための図である。

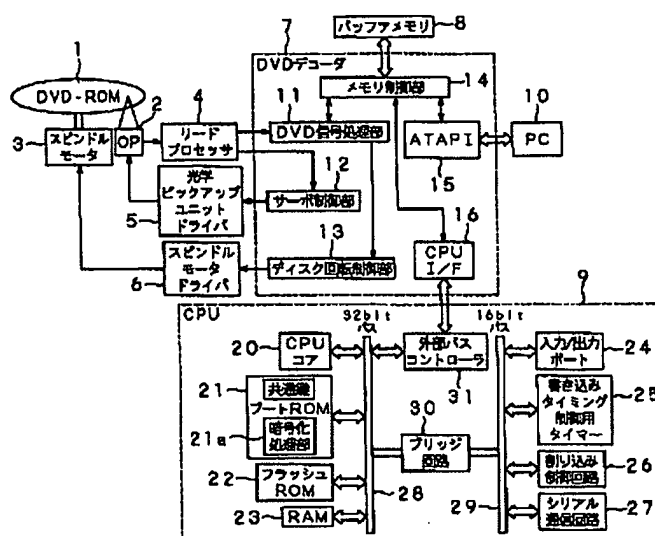
【図１４】本発明の第３の実施の形態として示すDVD-ROMドライブの構成を説明するためのブロック図である。

1 DVD-ROM (Digital Versatile Disc-Read Only Memory)、2 光学ピックアップユニット、3 スピンドルモータ、4 リードプロセッサ、5 光学ピックアップユニットドライバ、6 スピンドルモータドライバ、7 DVDデコーダ、8 バッファメモリ、9 CPU (Central Processing Unit)、20 CPUコア、21 ブートROM (Read Only Memory)、21a 暗号化処理部、22 フラッシュROM、23 RAM (Random Access Memory)、31 外部バスコントローラ

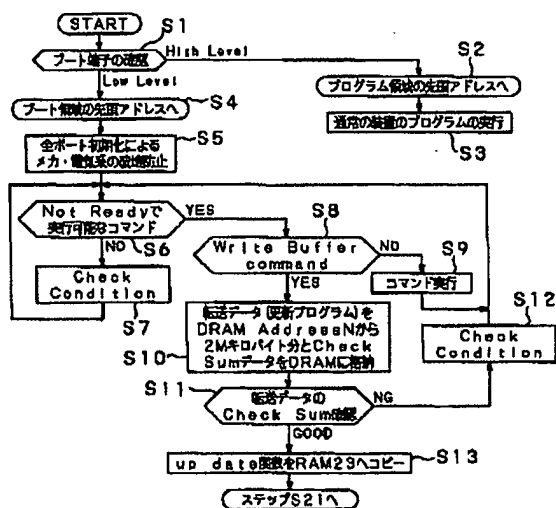
【图 20】



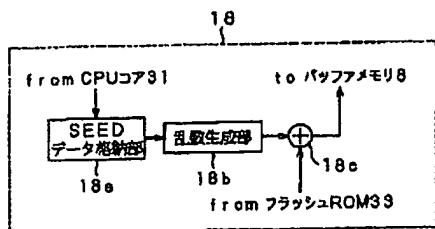
【図1】



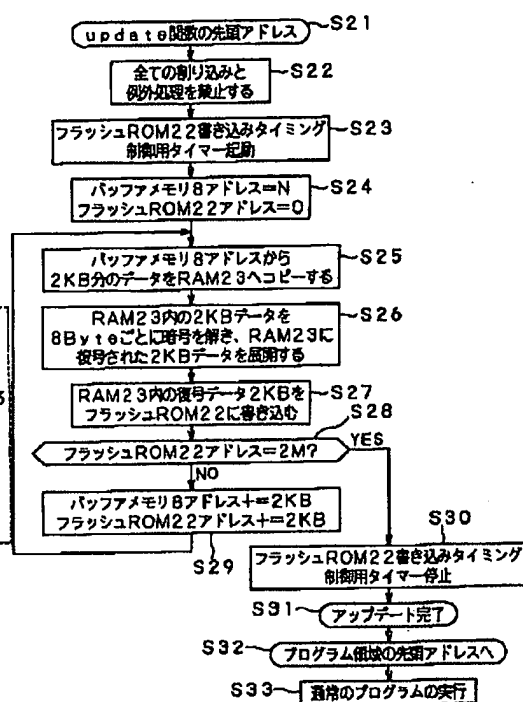
【図3】



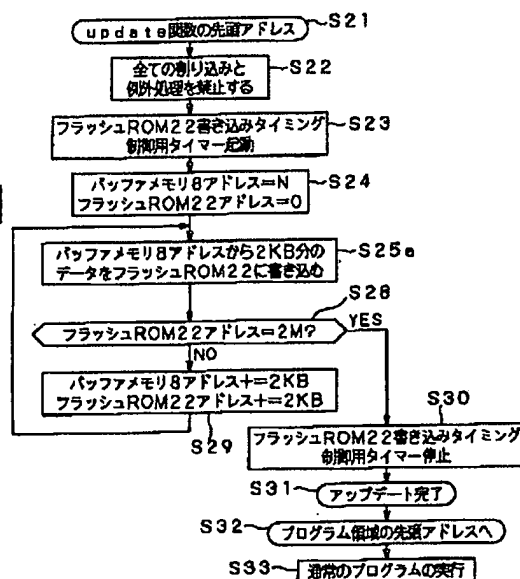
【図10】



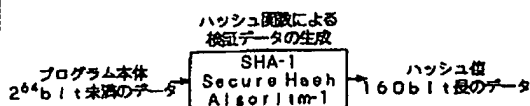
【図4】



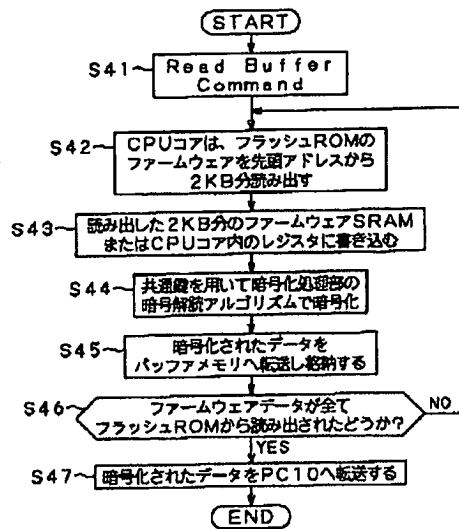
【図5】



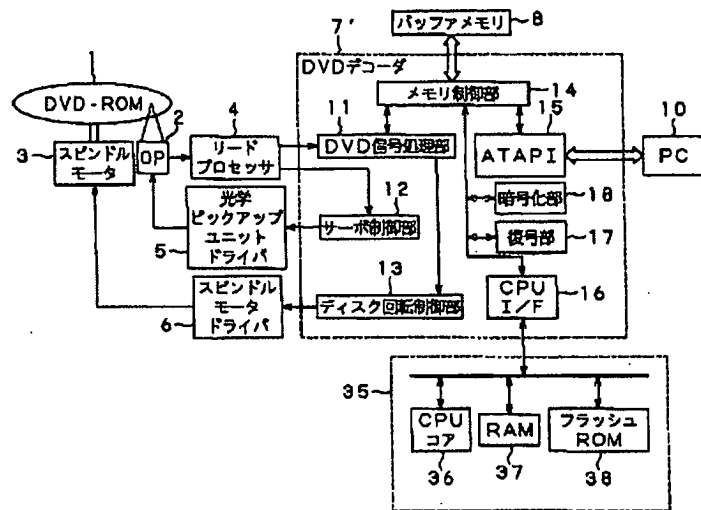
【図21】



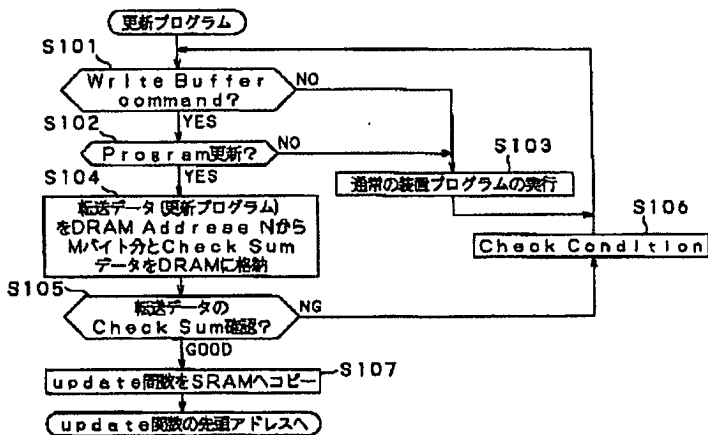
【図6】



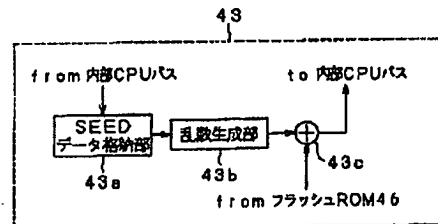
【図8】



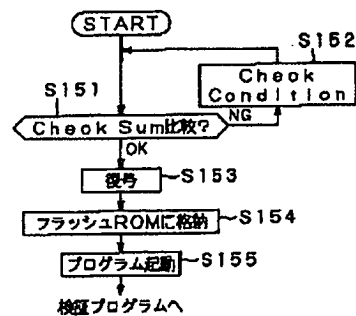
【図11】



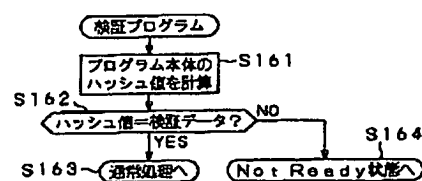
【図15】



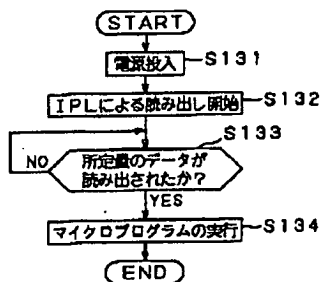
【図18】



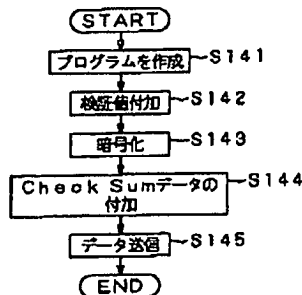
【図19】



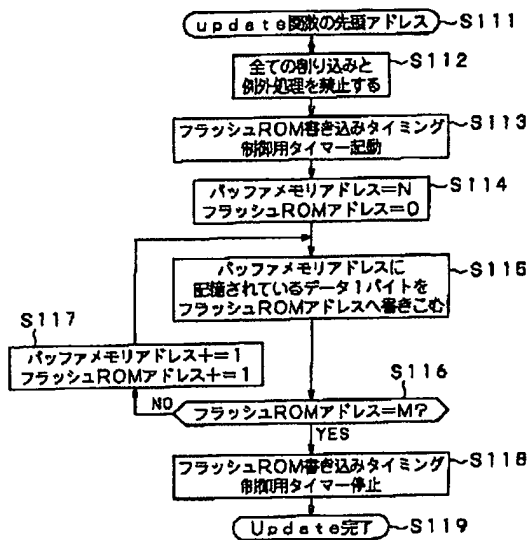
【図16】



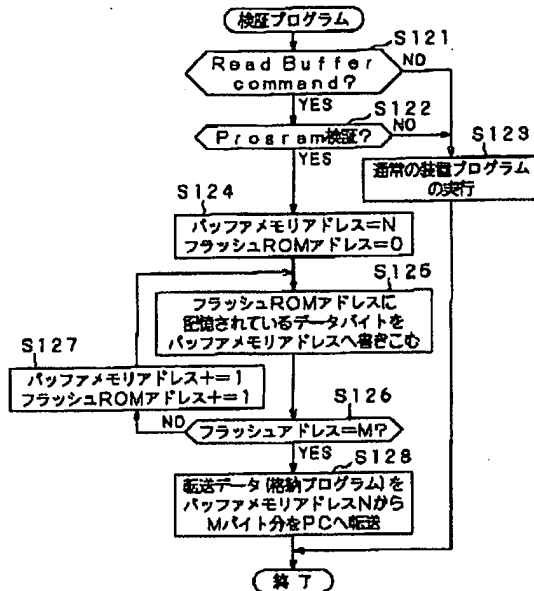
【図17】



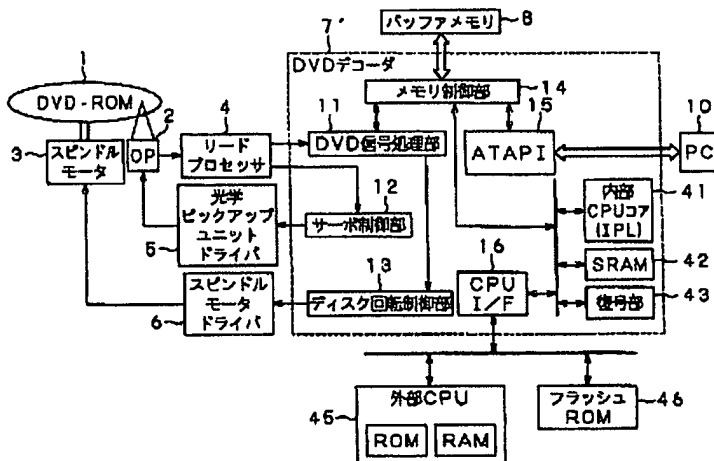
【図12】



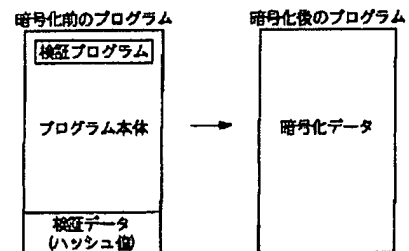
【図13】



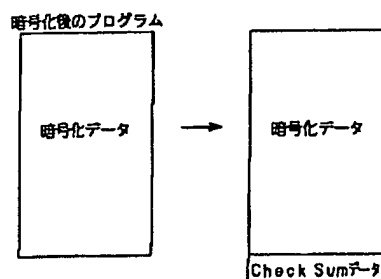
【図14】



【図22】



【図23】



フロントページの続き

Fターム(参考) SB017 AA08 CA15
SB076 FA00
5J104 EA18 NA02 NA12